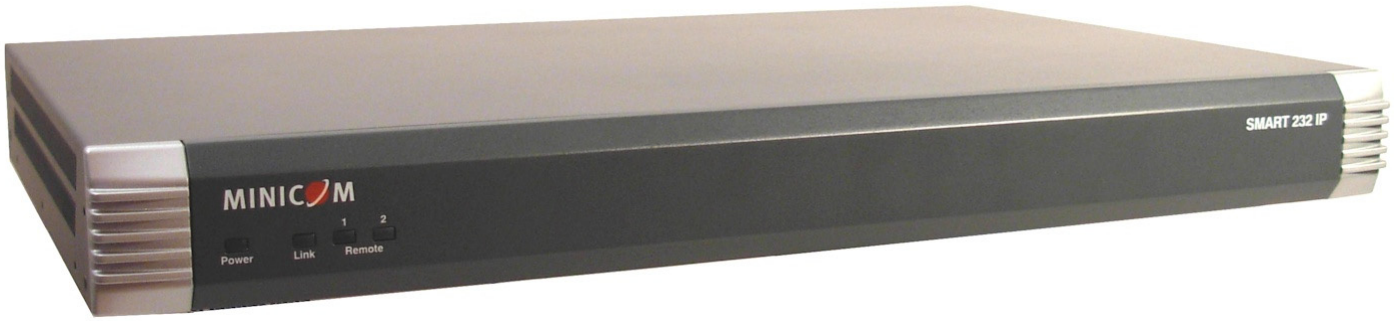
Smart 216/232 IP

User Guide



www.minicom.com

International HQ

Jerusalem, Israel

Tel: + 972 2 535 9666

minicom@minicom.com

North American HQ

Linden, NJ, USA

Tel: + 1 908 486 2100

info.usa@minicom.com

Technical Support – support@minicom.com

5UM20184 V2.0 4/11

Legal Notice

This manual and the software described in it are furnished under license, and may be used or copied only in accordance with the terms of such license. The content of this manual is provided for informational use only, and is subject to change without notice. It should not in and of itself be construed as a commitment by Minicom Advanced Systems Limited, which assumes no responsibility of liability for any errors or inaccuracies that may appear in this book.

The software that accompanies this manual is licensed for use by the Licensee only, in strict accordance with the software license agreement, which the Licensee should read carefully before commencing use of the software. Except as permitted by the license, no part of this publication may be reproduced, stored in retrieval system, or transmitted in any form of by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Minicom Advanced Systems Limited.

About this Document

This document provides installation and operation instructions for the Smart 216/232 IP system, produced by Minicom Advanced Systems Limited. It is intended for system administrators and network managers.

Chapters and Their Contents

1	**Introduction**	Provides an introduction to the document, Smart 216/232 IP product overview, features and benefits of Smart 216/232 IP, client computer operating system requirements, technical precautions, trademarks, and terminology used in the document. It also describes how to safely handle the device, provide feedback on the user guide, and WEEE Information for Minicom Customers and Recyclers.	Pg. 11
2	**Installation**	Lists Smart 216/232 IP system components, describes the functionalities of the Smart 216/232 IP elements, and provides instructions for rack mounting the unit and connecting the system.	Pg. 13
3	**Configuring the Network**	Provides instructions for logging into the Web configuration interface, configuring the device ID, IP address, and Centralized Management settings, adding, editing, removing, and blocking system Users, configuring the KVM switch, Serial port, security, user targets, system date and time, power outlets, and power device settings. It also provides instructions for installing an SSL certificate, upgrading firmware, upgrading RICCs/ROCs, restoring factory settings, backing up and restoring configuration data, and saving changes and logging out.	Pg. 24
4	**Conducting a Remote Session**	Describes how to start a remote session, set the session profile, full screen mode, view system information, adjust video settings, power manage target servers, manage keyboard sequences, synchronize mouse pointers, switch to a different server or device, and disconnect the remote session.	Pg. 52
5	**Managing the Events Log**	Describes how to view, reload, clear, and save the Events Log.	Pg. 74
6	**Troubleshooting – Restoring Factory Settings**	Describes how to restore the device to its factory settings using a USB drive.	Pg. 76
7	**Operating the Smart**	Describes how to operate Smart 216/232 IP using the	Pg. 77

	216/232 IP Switching System Locally	OSD.	
8	**Technical Specifications**	Lists and describes Smart 216/232 IP specifications.	Pg. 84
9	**Video Resolution and Refresh Rates**	Lists video resolutions and refresh rates.	Pg. 84

Style Conventions

Convention	Used for
Verdana	Regular text.
Arial Bold	Names of menus, commands, buttons, and other elements of the user interface.
Arial Italics	Special terms, the first time they appear.
`Monospace`	Text entered by the user.
	Notes, which offer an additional explanation or a hint on how to overcome a common problem.
	Warnings, which indicate potentially damaging user operations and explain how to avoid them.

Table of Contents

TABLE OF FIGURES IX

1 INTRODUCTION 11

1.1 PRODUCT OVERVIEW 11

1.1.1 Features and Benefits 11

1.2 TERMINOLOGY 12

1.3 COMPATIBILITY 12

1.4 CLIENT COMPUTER OPERATING SYSTEM 12

1.5 TECHNICAL PRECAUTIONS 12

1.6 SAFETY 13

1.7 USER GUIDE FEEDBACK 13

1.8 TRADEMARKS 13

1.9 WEEE COMPLIANCE 13

2 INSTALLATION 15

2.1 OVERVIEW 15

2.2 SYSTEM COMPONENTS 15

2.2.1 The Smart 216/232 IP Unit 15

2.3 PRE-INSTALLATION GUIDELINES 17

2.4 RACK MOUNTING THE SMART 216/232 IP UNIT 17

2.4.1 Rack Mounting Safety Considerations 17

2.4.2 Mounting the Unit 18

2.5 CONNECTING THE SYSTEM 19

2.6 CONNECTING TO THE SERVERS 20

2.6.1 Connecting a ROC PS/2 20

2.6.2 Connecting a ROC USB 21

2.7 CONNECTING TO THE NETWORK 22

2.8 CONNECTING THE CAT5 CABLES 22

2.9 CONNECTING THE KVM CONSOLE 22
2.10 CONNECTING THE POWER SUPPLY 23
3 CONFIGURING THE NETWORK 24
3.1 BOOT-UP PROCESS 24
3.2 LOGGING ONTO THE WEB CONFIGURATION INTERFACE 25
3.2.1 Web Configuration Interface Tabs 27
3.2.2 Web Configuration Toolbar Buttons 28
3.3 CHANGING YOUR PASSWORD 28
3.4 CONFIGURING THE NETWORK SETTINGS 29
3.4.1 Configuring Device ID Settings 29
3.4.2 Configuring the Device IP Address 30
3.4.3 Configuring Centralized Management Settings 30
3.5 CONFIGURING USER SETTINGS 31
3.5.1 Adding a User 31
3.5.2 Deleting User(s) 33
3.5.3 Blocking a User 33
3.5.4 Editing User Information 33
3.6 CONFIGURING THE KVM SWITCH 34
3.7 CONFIGURING THE SERIAL PORT SETTINGS 36
3.8 CONFIGURING THE SECURITY SETTINGS 36
3.9 CONFIGURING USER TARGETS 39
3.10 CONFIGURING THE SYSTEM DATE AND TIME 40
3.11 CONFIGURING POWER DEVICES 41
3.11.1 Editing a Power Device 42
3.11.2 Removing a Power Device 43
3.12 CONFIGURING POWER OUTLETS 43
3.13 PERFORMING ADDITIONAL CONFIGURATION OPERATIONS 44
3.13.1 Installing an SSL Certificate 44
3.13.2 Upgrading Firmware 45
3.13.3 Upgrading RICCs/ROCs 46
3.13.4 Restoring Factory Settings 47

3.13.5 Backing Up and Restoring 48
3.14 Reloading a Page 49
3.15 Saving Changes and Logging Out 49
4 CONDUCTING A REMOTE SESSION 52
4.1 Starting a Remote Session 52
4.1.1 Remote Session Toolbar Buttons 54
4.2 Sharing a Remote Session 55
4.2.1 Exclusive Session 56
4.3 Displaying the Toolbar 56
4.4 Setting the Session Profile 56
4.4.1 Full Screen Mode 57
4.5 Verifying Remote Presence Solutions Information 58
4.6 Changing the Video Performance Settings 59
4.7 Adjusting the Video 60
4.7.1 Refreshing the Video Image 60
4.7.2 Automatically Adjusting the Video Image 61
4.7.3 Manually Adjusting Video Settings 61
4.8 Power Managing the Target Servers 63
4.9 Managing Keyboard Sequences 63
4.9.1 Adding a Keyboard Sequence 64
4.9.2 Recording a New Custom Key 65
4.9.3 Editing a Key Sequence 66
4.9.4 Deleting Key Sequence(s) 66
4.10 Synchronizing Mouse Pointers 67
4.10.1 Manually Synchronizing the Mouse 67
Selecting the Mouse Mode 69
Relative Mouse Position Mode 70
4.10.2 Aligning the Mouse Pointers 72
4.10.3 Calibrating Mouse Pointers 72
4.11 Switching to a Different Server/Device 73
4.12 Disconnecting the Remote Session 73
5 MANAGING THE EVENTS LOG 74

5.1 VIEWING THE EVENTS LOG 74
5.2 RELOADING THE EVENTS LOG 74
5.3 SAVING THE EVENTS LOG 75
5.4 CLEARING THE EVENT LOG 75
6 TROUBLESHOOTING – RESTORING FACTORY SETTINGS 76
7 OPERATING THE SMART 216/232 IP SWITCHING SYSTEM LOCALLY .. 77
7.1 DISPLAYING THE OSD 77
7.2 NAVIGATING THE OSD 77
7.3 SELECTING A COMPUTER 78
7.4 POWER MANAGING A SERVER 78
7.5 MOVING THE CONFIRMATION LABEL (F1) 79
7.6 TUNING (F5) 79
7.7 CONFIGURING THE OSD SETTINGS (F2) 80
7.7.1 Changing the Network Parameters 81
Configuring the Device IP Address 81
Configuring AccessIT Centralized Management Settings 81
7.7.2 Changing the OSD Hotkey 82
7.7.3 Changing the Keyboard Language 82
7.7.4 Inputting and Updating DDC Information (F10) 82
7.7.5 Saving Changes to Settings 83
8 TECHNICAL SPECIFICATIONS 84
9 VIDEO RESOLUTION AND REFRESH RATES 86

Table of Figures

Figure 1 – Smart 216 IP Unit Front Panel 15
Figure 2 – Smart 216 IP Unit Rear Panel 16
Figure 3 – Smart 232 IP Rear Panel 16
Figure 4 – Bracket Positions 18
Figure 5 – Bracket Connected for Rear Facing 19
Figure 6 – Smart 216/232 IP System Overview 19
Figure 7 – ROC PS/2 20
Figure 8 – ROC USB 20
Figure 9 – ROC PS/2 Connections 21
Figure 10 – ROC USB 22
Figure 11 – OSD Main Window 25
Figure 12 – Settings Window 25
Figure 13 – Web Page 26
Figure 14 – Logon Page 26
Figure 15 – Network Configuration – Device Tab 27
Figure 16 – Change Password Page 29
Figure 17 – Users Page 32
Figure 18 – Add User Page 32
Figure 19 – Delete User Confirmation 33
Figure 20 – Edit User Page 34
Figure 21 – KVM Switch Configuration Page for Smart 232 IP 35
Figure 22 – Serial Port Page 36
Figure 23 – Security Page 38
Figure 24 – User Targets Page 40
Figure 25 – Date and Time Page 41
Figure 26 – Power Devices Page 41
Figure 27 – Add PDU Page 41
Figure 28 – Added Power Devices 42
Figure 29 – Edit PDU Page 42
Figure 30 – Delete PDU Confirmation Page 43
Figure 31 – Power Outlets Page 43
Figure 32 – Assigning Servers to Power Outlets Page 44
Figure 33 – SSL Certificate Page 45
Figure 34 – Device Version Upgrade Page 46
Figure 35 – Reboot Confirmation Page 46
Figure 36 – RICCs/ROCs Upgrade Page 47
Figure 37 – Restore Factory Settings Page 48
Figure 38 – Backup/Restore Data Page 49
Figure 39 – Device Reboot Confirmation Message 50

Figure 40 – Save Succeeded Message 50
Figure 41 – Device Rebooting Progress Box 50
Figure 42 – Logon Page after Rebooting 51
Figure 43 – Server Targets 53
Figure 44 – Remote Session Page 54
Figure 45 – Shared Remote Session 55
Figure 46 – Session Profile Dialog Box 57
Figure 47 – Remote Presence Solutions Information 58
Figure 48 – Performance Settings 60
Figure 49 – Video Adjust Progress 61
Figure 50 – Manual Video Adjustments Controls 62
Figure 51 – Power Menu 63
Figure 52 – Special Key Manager 64
Figure 53 – Add a Predefined Key Dialog Box 65
Figure 54 – Record Macro Box 66
Figure 55 – Delete Key(s) Confirmation Box 67
Figure 56 – Relative Mouse Settings 68
Figure 57 – Absolute Mouse Settings 69
Figure 58 – Windows 7 Mouse Properties 70
Figure 59 – Mouse Emulation Box 71
Figure 60 – Events Log 74
Figure 61 – Clear Events Confirmation Window 75
Figure 62 – OSD Main Window 77
Figure 63 – Power Control Dialog Box 78
Figure 64 – Power Prompt 79
Figure 65 – Image Tuning Label 80
Figure 66 – OSD Settings Window 80

1 Introduction

Congratulations on adding Smart 216/232 IP to your remote access tools.

This document provides installation and operation instructions for Minicom's Smart 216/232 IP. It is intended for system administrators and network managers, and assumes that readers have a general understanding of networks, hardware, and software.

Chapter 3 and Chapter 4 of this guide describe how to configure and operate the Smart 216/232 IP system remotely over IP. Chapter 7 explains how to operate the Smart 216/232 IP switching system locally through the On Screen Display (OSD).

1.1 Product Overview

The Smart 216/232 IP system extends your KVM (keyboard, video, and mouse) from any computer or server over TCP/IP via LAN, WAN, or Internet connection. This enables two remote users to simultaneously control, monitor, and manage up to 16/32 remote (PS/2, USB) servers from wherever they are, inside or outside the organization. Simultaneously, one local user can also access the servers. Simultaneously, two more remote users can operate serial devices, such as routers or managed network switches. Alternatively, one more user can use a PDU.

Smart 216/232 IP is a cost-effective hardware solution, for secure, remote KVM access and control of 16/32 computers/servers from the BIOS level – independent of the OS.

Smart 216/232 IP is based on Minicom's innovative ROC technology, in which each computer/server is directly connected to the switch via ROC dongles using only a standard CAT5 cable at a distance of up to 30 m / 100 ft in a star configuration. No external power is needed at the remote ROC.

The Smart 216 IP and Smart 232 IP are functionally the same. The Smart 216 IP has 16 Server ports; the Smart 232 IP has 32 Server ports.

1.1.1 Features and Benefits

Smart 216/232 IP has the following features and benefits:

- **BIOS level control** to any server's brand and model, regardless of the server condition and network connectivity. Covers the entire spectrum of crash scenarios.
- **Compatible** with all major operating systems. Supports many hardware and software configurations for the remote client and the Target server computers, as well as the KVM switch in use.

- **Web-based control** – Browser based control to a target server from any location, via a secured standard IP connection.
- **Security** – Supports the highest security standards for encryption (256-bit AES and HTTPS) and authentication for remote user and advanced OSD management, with multi-layer security for the local user.
- **Centralized Management** – Can be controlled by Minicom's Centralized Management system – AccessIT, for centralized over-IP management of distributed data center locations.

1.2 Terminology

The following table describes terms used in this guide.

Term	Definition
Target server	The computer/server that is accessed remotely via Smart 216/232 IP
Client computer	The PC running a remote Smart 216/232 IP session
Remote session	The process of accessing and controlling target servers connected to Smart 216/232 IP from a user workstation

1.3 Compatibility

Smart 216/232 IP is compatible with:

- PS/2, SUN, and USB computers/servers
- VGA, SVGA, and XGA monitors
- Windows, Linux, UNIX, and other major operating systems

1.4 Client Computer Operating System

The client computer operating system must be one of the following:

- Windows 2000 or later, with Firefox 3 or Internet Explorer 32-bit 7.0 or later version
- Linux with Firefox 3; 128-bit encryption support is required

1.5 Technical Precautions

This equipment generates radio frequency energy, and if not installed in accordance with the manufacturer's instructions, may cause radio frequency interference.

This equipment complies with Part 15, Subpart J of the FCC rules for a Class A computing device. This equipment also complies with the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications. These above rules are designed to provide reasonable protection against such interference when operating the equipment in a commercial environment. If operation of this equipment in a residential area causes radio frequency interference, the user, and not Minicom Advanced Systems Limited, will be responsible.

Changes or modifications made to this equipment not expressly approved by Minicom Advanced Systems Limited could void the user's authority to operate the equipment.

1.6 Safety

The device must only be opened by an authorized Minicom technician. Disconnect the device from the power source and all cables from the device before service operation!

1.7 User Guide Feedback

Your feedback is very important to help us improve our documentation. Please email any comments to: ug.comments@minicom.com.

Please include the following information:

- Guide name
- Part number
- Version number (on the front cover)

1.8 Trademarks

All trademarks and registered trademarks are the property of their respective owners.

1.9 WEEE Compliance

This section provides WEEE Information for Minicom Customers and Recyclers.

Under the Waste Electrical and Electronic Equipment (WEEE) Directive and implementing regulations, when customers buy new electrical and electronic equipment from Minicom, they are entitled to:

- Send old equipment for recycling on a one-for-one, like-for-like basis (this varies depending on the country)
- Send back the new equipment for recycling when it ultimately becomes waste

Instructions for both customers and recyclers / treatment facilities wishing to obtain disassembly information are provided in our website www.minicom.com.

2 Installation

2.1 Overview

Install the Smart 216/232 IP system as follows:

1. Remove the Smart 216/232 IP system from the package, and check that all components are present and in good working condition.
2. Mount the Smart 216/232 IP unit in a rack.
3. Make all hardware connections between the power source, Smart 216/232 IP, services, network, and KVM console.
4. Power on the Smart 216/232 IP unit.

2.2 System Components

Before installing the Smart 216/232 IP system, verify that you have all the components on the following list, as well as any other items required for installation.

The Smart 216/232 IP system consists of:

- One Smart 216/232 IP (p/n 1SU70036) or one Smart 232 IP (p/n 1SU70037)
- One RS232 Download cable (p/n 5CB40419)
- ROCS - PS/2, USB (ordered separately)
- CAT5 cables (1.5 m provided)
- A rack mounting kit (p/n 5AC20247)

2.2.1 The Smart 216/232 IP Unit

The Smart 216/232 IP Unit front panel is illustrated in Figure 1.

Figure 1 – Smart 216 IP Unit Front Panel

The following table describes the functionality of the LEDS on the front panel of the Smart 216/232 IP.

LED	Functionality
Power LED	Indicates the state of the Smart 216/232 IP unit: Green indicates that the unit is powered on; Red indicates that the unit is powered off.
Remote 1, Remote 2 LEDs	Illuminate to indicate that a remote session is active.
Link	Illuminates to indicate that the unit is connected to the network.

The Smart 216 IP unit rear panel is illustrated in Figure 2; it has 16 server ports. The Smart 232 IP unit rear panel is illustrated in Figure 3; it has 32 server ports.

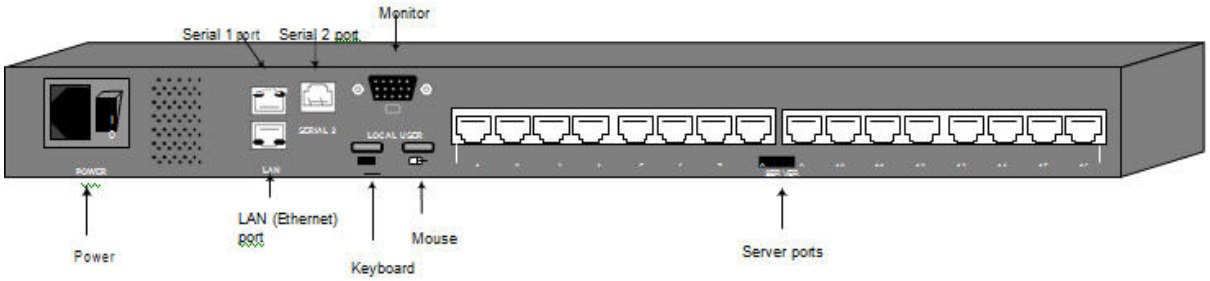


Figure 2 – Smart 216 IP Unit Rear Panel

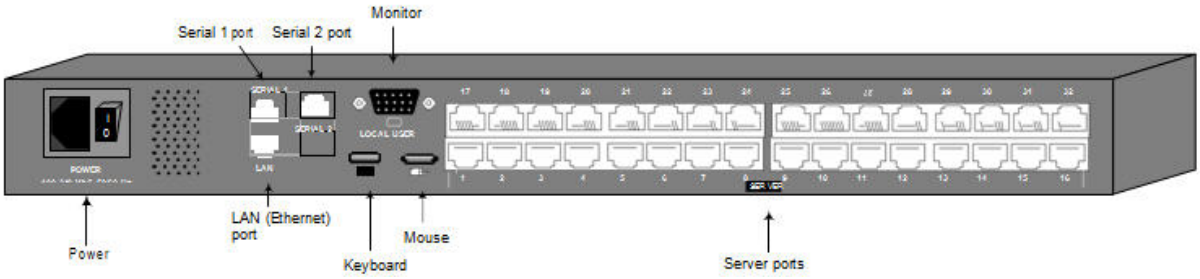


Figure 3 – Smart 232 IP Rear Panel

The following connector table describes the functionality of the ports on the rear panel of the Smart 216/232.

Port	Functionality
Console KVM	For connecting a keyboard, video, and mouse to operate the Smart 216/232 IP locally; optional.
Serial 1	For connecting the Smart 216/232 IP unit to any serial manageable devices, such as power management units and routers, via the RS232 cable. **Note:** Minicom's Serial Remote PowerSwitch must be connected to **Serial 1**.
Serial 2	For connecting the Smart 216/232 IP unit to any Serial device.

Port	Functionality
Flash	For updating firmware of the analogue part of the Smart 216/232 IP system - OSD, Switch, RICCs, and ROCs.
LAN	For connecting to the 10/100 Mbit Ethernet. The LED illuminates yellow when the unit is connected to LAN; green when a remote session is in progress.
Server ports	For connecting to the servers via ROCs.

2.3 Pre-Installation Guidelines

- Place cables away from fluorescent lights, air conditioners, and machines that are likely to generate electrical noise.
- Place the Smart 216/232 IP unit on a flat, clean and dry surface.
- The Smart 216/232 IP unit is not intended for connection to exposed outdoor lines.
- Ensure that the maximum distance between each computer and the Smart 216/232 IP unit, does not exceed 30 m / 100 ft for ROCs.

2.4 Rack Mounting the Smart 216/232 IP Unit

2.4.1 Rack Mounting Safety Considerations

When mounting Smart 216/232 IP onto a rack, avoid the following conditions:

- **Elevated operating ambient temperature** – The operating ambient temperature of the rack environment may be greater than the room ambient temperature. Therefore, take special care when installing the unit in a closed or multi-unit rack assembly that the environment is compatible with the maximum rated ambient temperature.
- **Reduced airflow** – Install the equipment in a rack in such a way that the amount of airflow required for safe operation is not compromised. Leave a gap of at least 5 cm / 2” on each side of Smart 216/232 IP.
- **Uneven mechanical loading** – Uneven loading can cause damage to the equipment or personal injury. Mount the equipment in the rack in such a way that a hazardous condition does not result due to uneven mechanical loading.
- **Circuit overloading** – When connecting the equipment to the supply circuit, make sure that the total power of all the components does not exceed the circuit capabilities. Overloading of circuits can affect over-current protection and supply wiring, potentially resulting in fire and shock hazards.

- **Unreliable earthing** – Maintain reliable earthing of rack-mounted equipment. Pay attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

2.4.2 Mounting the Unit

You can connect the Smart 216/232 IP unit to a server rack, using the supplied rack mounting kit. The brackets can be placed in two possible positions, as illustrated in the following figure.

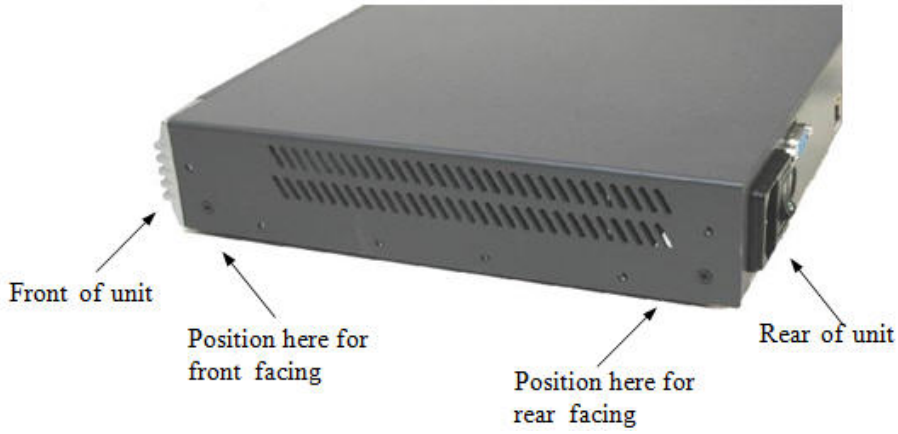


Figure 4 – Bracket Positions

➔ **To rack mount the Smart 216/232 IP unit:**

1. Place the brackets on the unit in either of the following ways:
   - Towards the front of the unit so that the unit can be mounted front facing
   - Towards the rear of the unit so that the unit can be mounted rear facing

   Figure 5 illustrates the bracket connected for rear facing.
2. Screw the bracket to the Smart 216/232 IP unit using the screws provided.

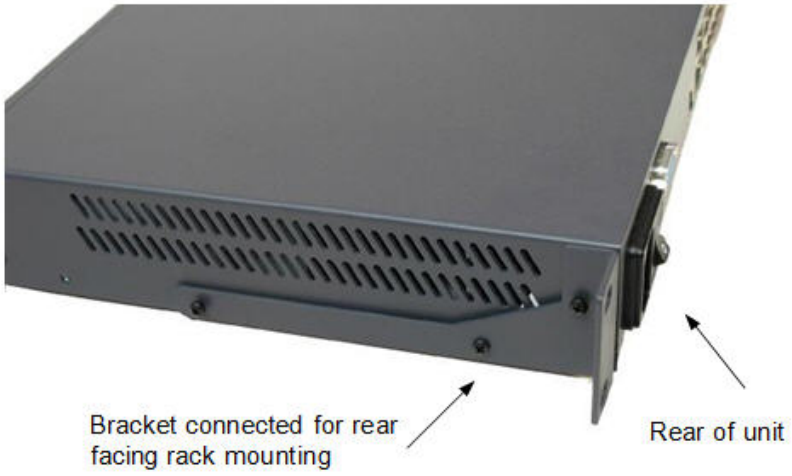


Figure 5 – Bracket Connected for Rear Facing

3. Install the Smart 216/232 IP nit into the server rack by connecting the bracket to the rack with screws, according to the rack manufacturer's instructions.

2.5 Connecting the System

Figure 6 illustrates the Smart 216/232 IP system overview.

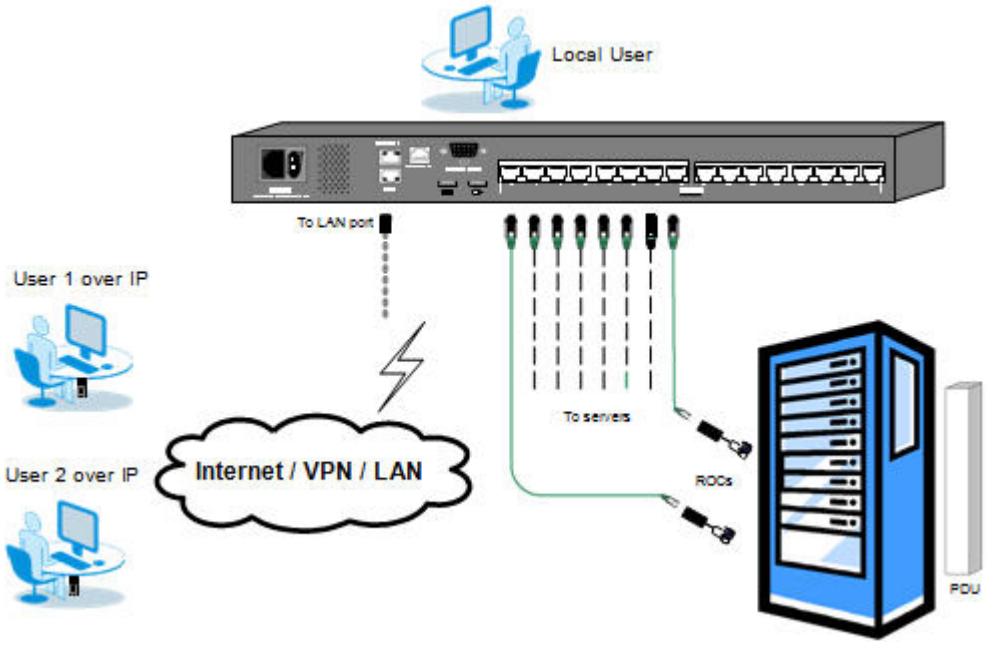


Figure 6 – Smart 216/232 IP System Overview

2.6 Connecting to the Servers

Each computer/server is directly connected to the Smart 216/232 IP via an appropriate ROC using a CAT5 cable in star configuration. No external power is needed at the remote ROCs. The ROCs draw their power from the computer's keyboard port (ROC PS/2, SUN) or from the USB port (ROC USB). Figure 7 and Figure 8 illustrate the ROC PS/2 and ROC USB.

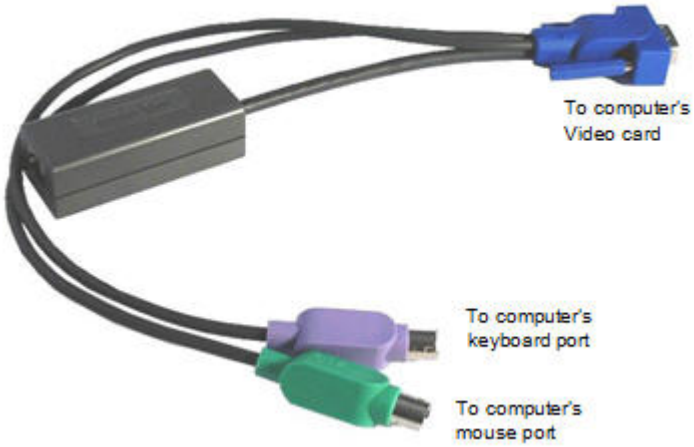


Figure 7 – ROC PS/2

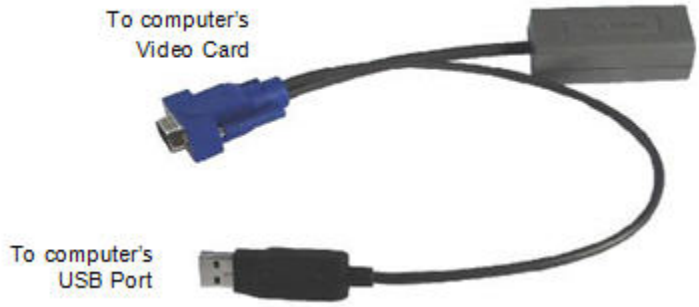


Figure 8 – ROC USB

2.6.1 Connecting a ROC PS/2

The following figure illustrates the ROC PS/2 connections.

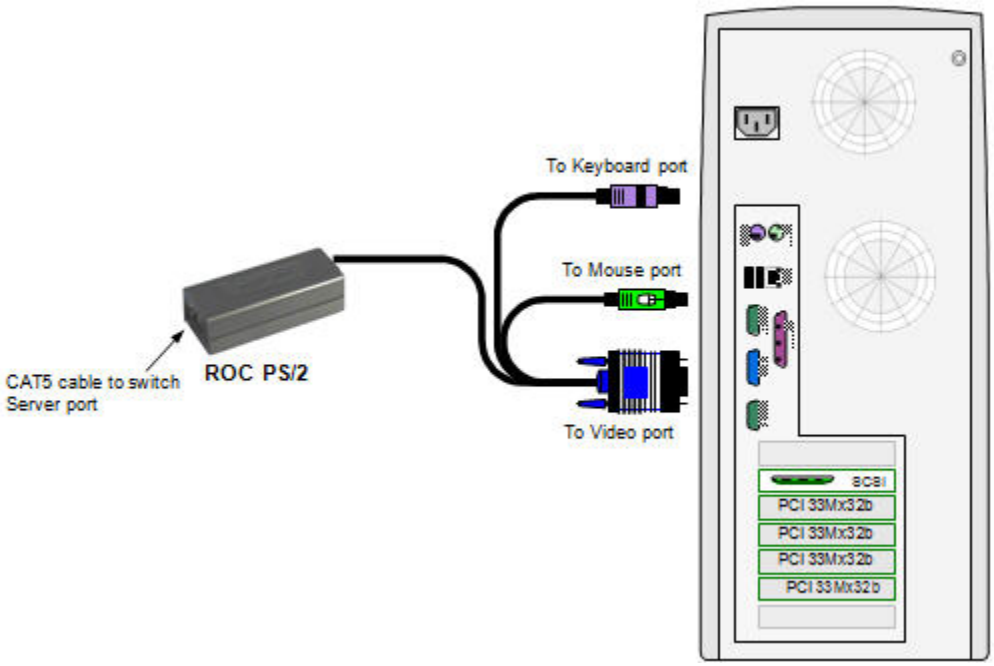


Figure 9 – ROC PS/2 Connections

You can connect the ROC PS/2 to a powered on computer, by performing the steps of the following procedure in order.

➔ **To connect the ROC PS/2 to a powered on computer:**

1. Connect the Mouse connector to the computer's Mouse port.
2. Connect the Keyboard connector to the computer's Keyboard port.
3. Connect the Screen connector to the computer's Video card.

Failure to connect in the above order while the server is running may lead to the mouse malfunctioning until the server is rebooted.

2.6.2 Connecting a ROC USB

The ROC USB supports Windows 98 SE and later, MAC, SUN, and SGI, and all modern Linux distributions.

The following figure illustrates the ROC USB and its connections.

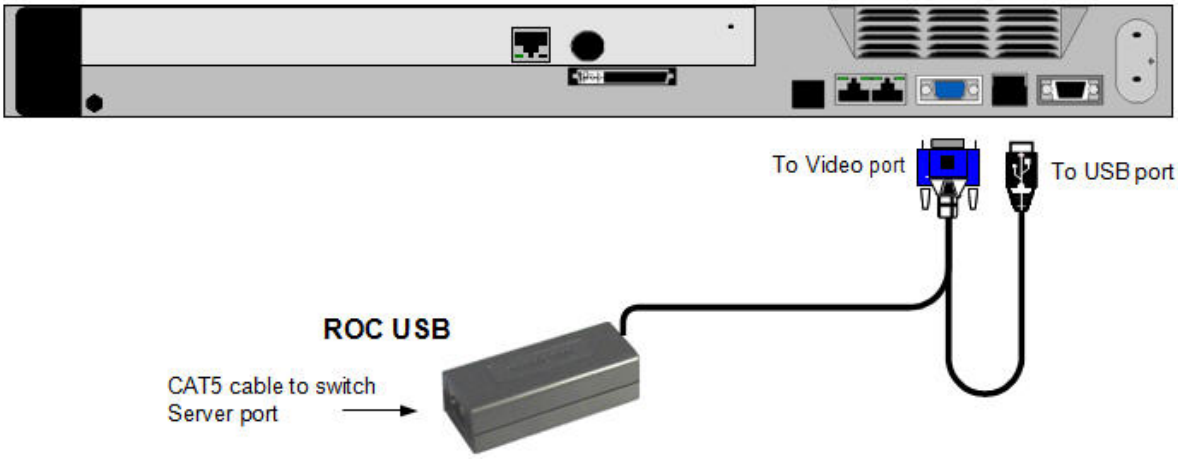


Figure 10 – ROC USB

➔ **To connect the ROC USB:**

1. Connect the Screen connector to the computer's video card.
2. Connect the USB connector to the computer's USB port.

2.7 Connecting to the Network

Before powering on Smart 216/232 IP, you can connect the Smart 216/232 IP to the network.

➔ **To connect the Smart 216/232 IP to the network:**

1. Connect the network cable to the LAN port of the Smart 216/232 IP.

2.8 Connecting the CAT5 Cables

Perform the following procedure for each computer to which you want to connect CAT5 cables.

➔ **To connect the CAT5 cables:**

1. Connect one connector to the ROC RJ45 port.
2. Connect the other connector to one of the Smart 216/232 IP computer ports.

2.9 Connecting the KVM Console

You can connect a KVM console to Smart 216/232 IP, in order to operate the system locally.

➔ **To connect a KVM console to Smart 216/232 IP:**

1. Connect the monitor's connector to the Smart 216/232 IP's Monitor port.
2. Connect the keyboard's USB connector to the Smart 216/232 IP's USB Keyboard port.
3. Connect the mouse's USB connector to the Smart 216/232 IP's USB Mouse port.

2.10 Connecting the Power Supply

➔ **To connect the power supply to Smart 216/232 IP:**

1. Using the power cord provided, connect Smart 216/232 IP to a socket outlet with a grounding connection.

Only use the power cord supplied with the unit.

2. Switch on Smart 216/232 IP.

3 Configuring the Network

After the system has been installed and all connections have been made, you must configure the Smart 216/232 IP system as follows:

1. Configure Smart 216/232 IP's network settings, which includes configuring:
   - Device ID settings
   - Smart 216/232 IP's IP address
   - Centralized Management
2. Add, edit, remove, and block system Users.
3. Configure the KVM switch settings.
4. Configure the Serial port settings.
5. Configure the security settings.
6. Configure the user targets.
7. Configure the system date and time.
8. Configure power devices.
9. Configure power outlets.

You can also perform the following additional operations, as required:

1. Install an SSL certificate.
2. Upgrade firmware.
3. Upgrade RICCs/ROCs.
4. Restore factory settings.
5. Back up and restore configuration data.

3.1 Boot-Up Process

By default, Smart 216/232 IP boots with an automatically assigned IP address from a DHCP (Dynamic Host Configuration Protocol) server on the network. The DHCP server assigns the Smart 216/232 IP a valid IP address, gateway address, and subnet mask.

You can identify the IP address from the OSD at the local position. Also, where there is no DHCP server, you can set the IP address locally via the OSD, as described in the following procedure.

➔ **To set the IP address locally via the OSD:**

1. From the local keyboard, press **Shift** twice.

The OSD Main window appears.

Figure 11 – OSD Main Window

2. Press **F2**.

   The Settings window appears see Figure 12.

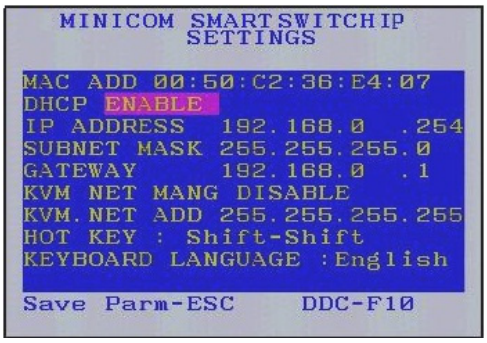


Figure 12 – Settings Window

3. In the Settings window, navigate downwards using the **Tab** key. At the bottom of the window, press **Tab** to go to the top of the window. Change settings by typing in the selected area or by pressing the spacebar – whichever is relevant.
4. If DHCP is disabled, in the Settings window, type the **IP Address**, **Subnet Mask**, and **Gateway**, as given by your Network Administrator.

   Otherwise, if a DHCP server is active on the same network to which Smart 216/232 IP is connected, DHCP provides automatic IP assignment.

5. Once the IP address is satisfactory, proceed to log onto the Web interface to complete the configuration.

3.2 Logging Onto the Web Configuration Interface

You can complete the initial setup of the Smart 216/232 IP system via the Web configuration interface.

Only one Administrator at a time can log onto the Web configuration interface. An idle timeout of 30 minutes terminates the session.

Before logging on the first time, verify that you have the latest Java installed on your computer. If not, you can download and install Java from: http://www.java.com/en/download/index.jsp

- **To log into the Web interface:**

1. Open your Web browser (Internet Explorer 7.0 / Firefox 3 or later).
2. Type the Smart 216/232 IP system IP address http://IP address/ or https://IP address/, and press **Enter**.

   The Web page appears.

Figure 13 – Web Page

3. Click **Log On**.

   Java installs. After installation has completed, the logon page appears.

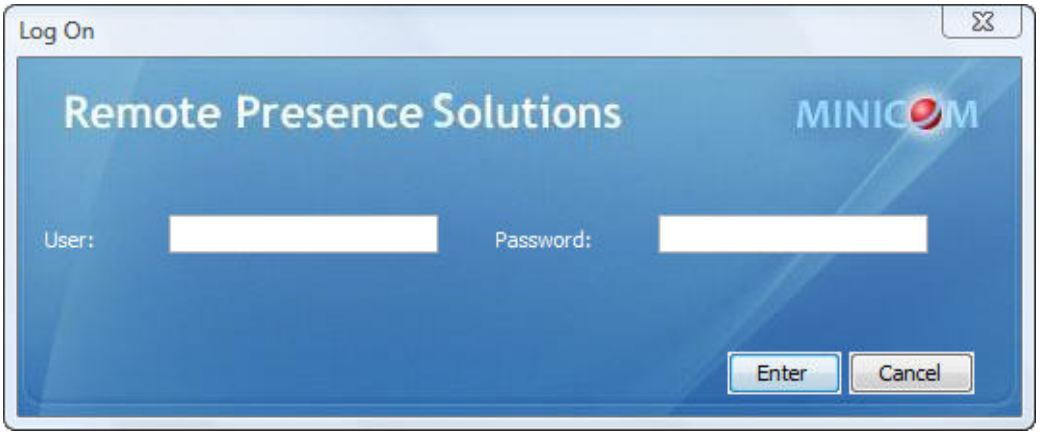


Figure 14 – Logon Page

4. In **User**, type the default Administrator name **admin** and in **Password**, type **access** (both lower case).

5. Click **Enter**.

   The Targets page opens, displaying all your available target servers (see Figure 43).

6. In the menu in the left pane, click

.

   The Network configuration page appears with the **Device** tab open.

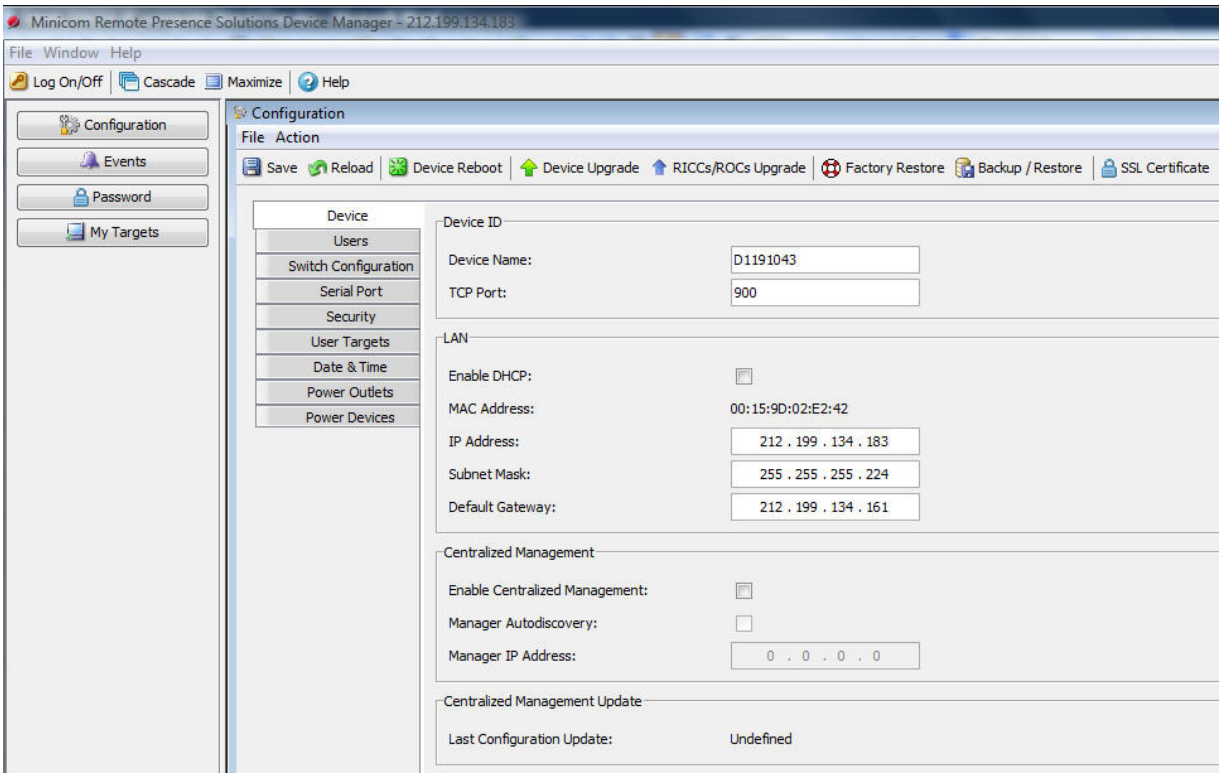


Figure 15 – Network Configuration – Device Tab

From the Configuration menu, you can configure the network, Users, Switch Configuration, Serial Port, Security, User Targets, Date & Time, Power Outlets, and Power Devices settings. **After making all configuration changes, you must click the**

button in the toolbar for the changes to go into effect.

3.2.1 Web Configuration Interface Tabs

The following table summarizes the Web configuration interface tabs.

Tab	Description
Device	For configuration of the device settings, IP address, and centralized management
Users	For adding, editing, deleting, and blocking system Users

Tab	Description
Switch Configuration	For configuration of the KVM switch settings
Serial Port	For configuration of the Serial port settings
Security	For configuration of the security settings
User Targets	For configuration of the access rights of each user to target servers
Date & Time	For configuring the system date and time
Power Outlets	For matching a server to each power outlet of all power devices defined in the system
Power Devices	For configuring the details of all power devices in the system

3.2.2 Web Configuration Toolbar Buttons

The following table describes the functionality of the Web configuration toolbar buttons.

Button	Functionality
Save	Saves the configuration changes
Reload	Reloads the device settings into the configuration page parameter settings
Device Reboot	Reboots the device
Device Upgrade	Upgrades the device firmware
RICCs/ROCs Upgrade	Upgrades the RICC/ROC firmware
Factory Restore	Restores the device with factory settings
Backup / Restore	Backs up or restores configuration data to/from a file
SSL Certificate	Installs the SSL certificate onto the device

3.3 Changing your Password

You can change your password, according to the set password policy.

➔ **To change the password:**

1. In the menu in the left pane, click Password.

   The Change Password page is displayed.

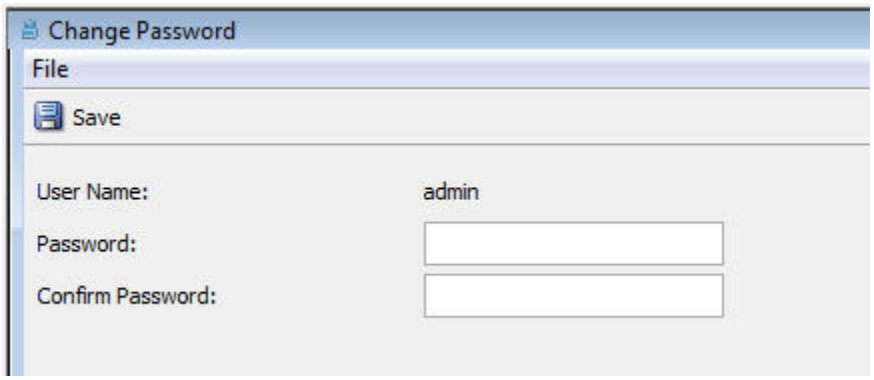


Figure 16 – Change Password Page

2. In **Password**, type a new password, according to the password naming conventions.
3. In **Confirm Password**, retype the new password.
4. Click Save.

   The new password is saved in the system. Use it next time you log on.

3.4 Configuring the Network Settings

On the network configuration page (see Figure 15), you can configure the following:

- Device ID
- Device IP address
- Centralized Management

Consult your Network Administrator for the network settings.

3.4.1 Configuring Device ID Settings

You can assign a name to the Smart 216/232 IP device, and select a TCP port.

The default device name consists of the letter 'D' followed by the 6-digit device number (D.N.), which is printed on the silver label on the underside of the Smart 216/232 IP box.

If the DHCP server is published in the DNS server, you can connect to the Smart 216/232 IP system using the device name, as follows: https://DeviceName.

You can select any TCP port from port # 800 to 65535. When managed by Centralized Management, the port number can be changed from the management interface, if needed.

Firewall or router security access list must enable inbound communication through the selected TCP port for the Smart 216/232 IP's IP address. (Default TCP port is 900; default Web interface TCP port is 443.)

For client computer access from a secured LAN, the selected ports should be open for outbound communication.

➔ **To configure Device ID settings:**

1. In **Device Name**, type a name for Smart 216/232 IP.
2. In **TCP Port**, type the number of the port (from 800 to 65535).

3.4.2 Configuring the Device IP Address

When a DHCP server is active on the same network to which Smart 216/232 IP is connected, the DHCP can provide automatic IP assignment. However, best practices recommend using MAC address reservations in the DHCP server to ensure that the IP address of the Smart 216/232 IP will not be changed.

Consult your Network Administrator regarding the use of the DHCP.

If you have access to the server, your configured (or default) Smart 216/232 IP device name will appear on the DHCP server's interface, making it easy to locate.

➔ **To configure the device IP address, do one of the following:**

- **Select automatic IP address assignment** – Select the **Enable DHCP** checkbox to enable a DHCP server that is active on the same network to which Smart 216/232 IP is connected, to provide automatic IP assignment.
- **Select manual IP address assignment** – Clear the **Enable DHCP** checkbox to disable the DHCP, and then type the **IP Address**, **Subnet Mask**, and **Default Gateway** for **LAN 1**, provided by your Network Administrator.

3.4.3 Configuring Centralized Management Settings

Minicom's Centralized Management IP-based systems ensure secure control of servers and network devices, and power and user administration in the data center environment. The Centralized Management systems combine out-of-band KVM via IP access with modern IT standards and requirements. They are the most comprehensive remote server maintenance solutions available in the market today.

➔ **To configure Centralized Management settings:**

1. Select the **Enable Centralized Management** checkbox to enable Smart 216/232 IP to be remotely managed by a Centralized Management system.

   When managed by Centralized Management, only Network Configuration is available from the Smart 216/232 IP configuration page. All other settings, such as Device Upgrade, Factory Restore, and SSL Certificate are disabled and are managed from Centralized Management.

2. Select the **Manager Auto Discovery** checkbox to cause the Centralized Management system to automatically detect Smart 216/232 IP, if they both reside on the same network segment.

   OR

   In **Manager IP Address**, type the static IP address of the Centralized Management Manager.

Although not required, it is recommended to type the **Manager IP Address** even if the Smart 216/232 IP resides on the same network segment as the Centralized Management Manager.

3.5 Configuring User Settings

An Administrator can add, edit, remove, and block Users.

There are two levels of user access:

- **Administrator** – has unrestricted access to all windows and settings, and can change the name and password of all users
- **User** – can access and control target servers, but cannot use advanced mouse settings and power cycle; cannot access the Web configuration interface

3.5.1 Adding a User

➔ **To add a User:**

1. From the configuration menu, select **Users**.

   The Users page opens and displays the existing Users.

Figure 17 – Users Page

2. Click the **Add** button.

   The Add User page appears.

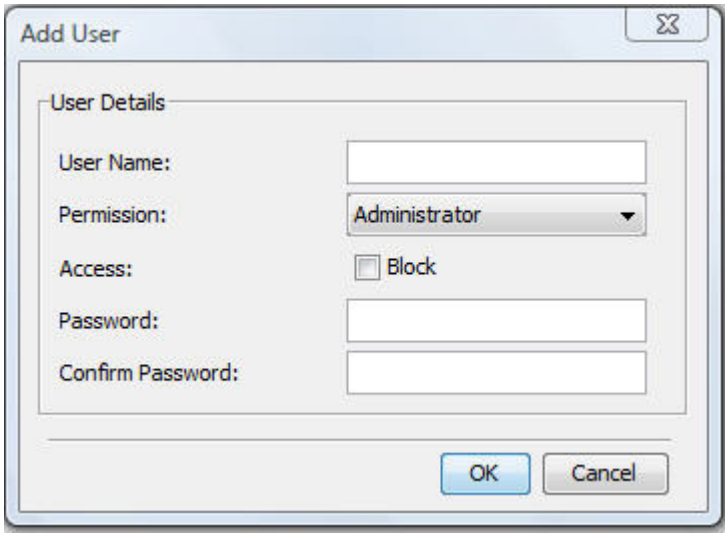


Figure 18 – Add User Page

3. Type a **User Name** and **Password**. The password must be at least six alphanumeric characters long and cannot include the user name, even if other characters are added.

The "special" characters **&**, **<**, **>**, and " cannot be used for either the user name or password.

The **User Name** and **Password** parameters depend on the security level chosen (see Section 3.8 on page 36).

4. In **Confirm Password**, retype the password.
5. In the **Permission** dropdown menu, select the permission type: **Administrator** or **User**.
6. Click **OK**.

   The User is added to the list of Users.

3.5.2 Deleting User(s)

You can delete one or multiple Users at a time from the system.

You cannot delete an Administrator who is logged onto the system.

➔ **To delete a User:**

1. In the **Users** page (see Figure 17), select User(s) to delete. Select a group of Users by selecting the first User in the group, pressing the **Shift** button, and then selecting the last User.
2. Click the **Delete** button.

   The Delete confirmation page appears.

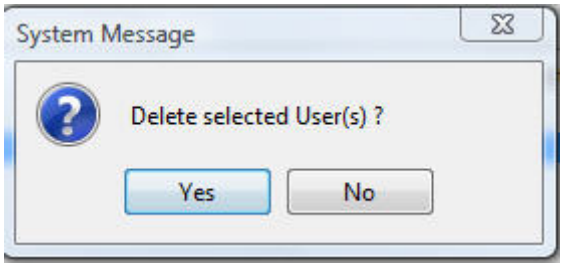


Figure 19 – Delete User Confirmation

3. Click **Yes**.

   The User(s) are deleted from the system.

3.5.3 Blocking a User

An alternative to deleting a User is blocking a User. This means that the User's name and password is stored, but the User is unable to access the system.

➔ **To block a User:**

1. In the **Add User** page (see Figure 18), in the **Access** parameter, select the **Block** checkbox.

3.5.4 Editing User Information

You can change any of the following User parameters: **Permission**, **Access**, and **Password**.

➔ **To edit User information:**

1. In the **Users** page (see Figure 17), select a User and click the **Edit** button.

The Edit User page appears, with the User's information in the parameters.

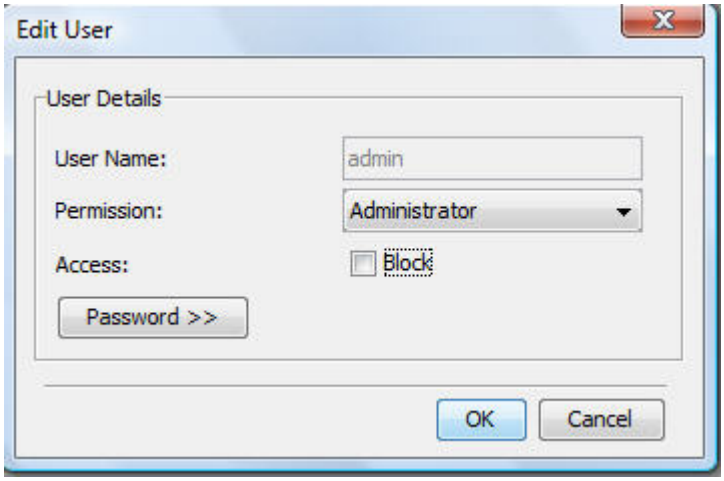
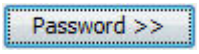


Figure 20 – Edit User Page

2. Change the **Permission** and/or **Access** as required.
3. To change the password, click  .

   The **Password** parameter opens. In the upper textbox, type the new password; in the lower textbox, confirm the new password.

You cannot change the password of an Administrator who is currently logged on to the system.

4. Click **OK**.

   The User page opens with the user information changed accordingly.

3.6 Configuring the KVM Switch

When a KVM switch is connected to the Smart 216/232 IP system, configure the following switch parameters:

- The names of the servers connected to the KVM switch – It is recommended to give the servers connected to Smart 216/232 IP unique names, so that users accessing the system can easily identify the servers.
- The number of POCs attached to those servers that are configured with POCs attached to them

➔ **To configure a KVM switch:**

1. From the configuration menu, select **Switch Configuration**.

The KVM Switch Configuration page appears.

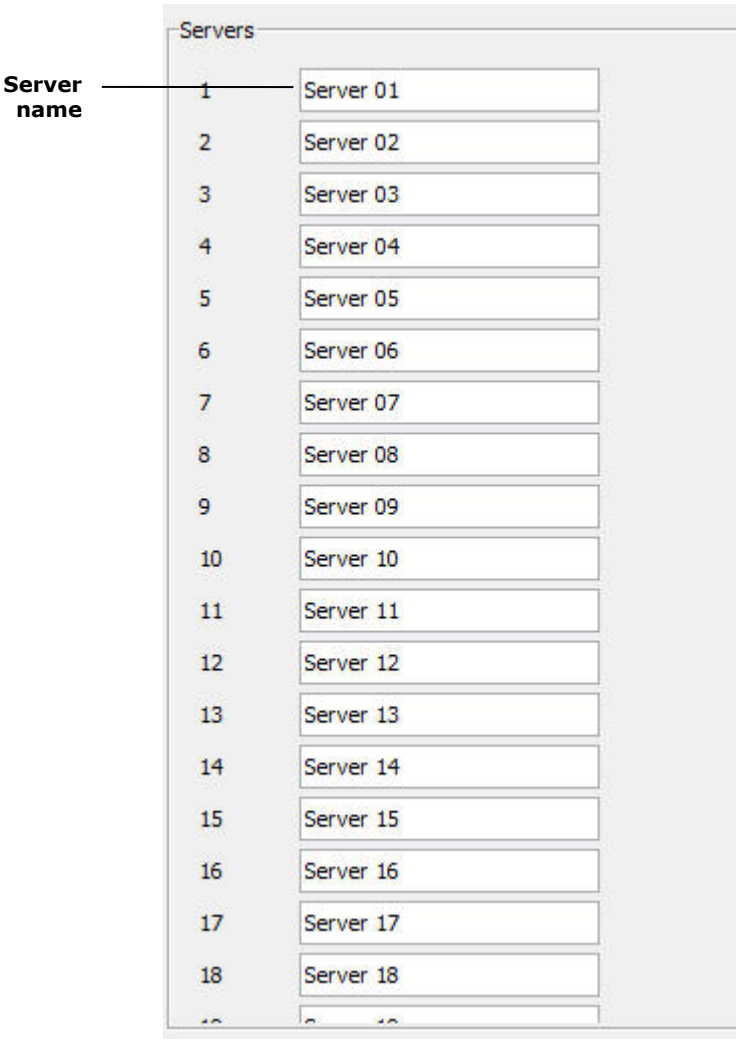


Figure 21 – KVM Switch Configuration Page for Smart 232 IP

The servers that are connected to the selected KVM switch, appear in the **Servers** section. The number of servers that appear corresponds to the number of ports in the KVM switch – 16 for Smart 216 IP; 32 for Smart 232 IP.

The following information is displayed for each potential server:

- The server number
- The server name

2. To change the name of a connected server, highlight the current server name, and type a new name.

3.7 Configuring the Serial Port Settings

When you have Serial device(s) connected to the system, you must configure the Serial Port settings of each device.

If you have a Minicom Serial Remote Power Switch, it must be connected to Serial Port 1.

➔ **To configure the serial port settings:**

1. From the configuration menu, select **Serial Port**.

   The Serial Port page appears.

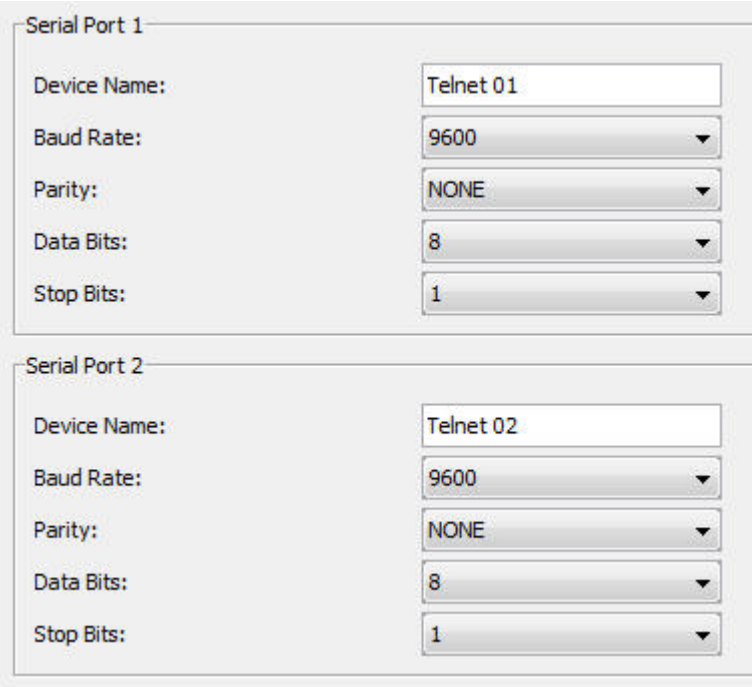


Figure 22 – Serial Port Page

2. For each serial device connected, type a **Device Name** and choose the correct device parameters.

3.8 Configuring the Security Settings

This section describes how to configure the security features, such as Account Blocking, Password Policy, Idle Timeout, and Serial Terminal Policy.

For local and remote users, you have the option of a standard or high security level of password. The following table describes both these options.

Standard Security Policy	High Security Policy
At least six characters	At least eight characters; must include at least one digit, one uppercase letter, and one of the following "special" characters: **!**, **@**, **#**, **$**, **%**, **^**, *, **()**, **_**, **-**, **+**, **=**, **[]**, ', **:**, **;**, **?**, /, or **{}**
Must not include the user name	Must not include the user name

For a local user, access to the OSD can be password enabled or disabled (default), with the option of a standard or high security level of password, as explained above.

User access permissions are the same regardless of whether access is done locally or remotely.

Serial Terminal Policy

The Smart 216/232 IP device enables you to control serial devices by connecting to them via the device's Web interface, as follows:

- Logging into the Smart 216/232 IP Web interface
- Clicking a serial port
- Connecting

This way, the Smart 216/232 IP internal SSH client is opened and used for the session.

Alternatively, you can bypass the Web interface and connect directly to the serial device itself. To do so, the Smart 216/232 IP device should be configured to "Enable direct SSH connection", which will redirect all serial communication messages to/from the connected device via a dedicated TCP port.

This will enable you to use your preferred SSH client to communicate directly to the serial device via the specified TCP port, opening and closing sessions autonomously without the need for a Web interface.

The default TCP ports used to operate Serial connections 1 and 2 are TCP ports 4001 and 4002 respectively.

Hence, when "Enable direct SSH connection" is selected:

1. Connect to the Serial device, by typing the IP address of the Smart 216/232 IP, followed by the TCP port number in your SSH client.
2. Log in to the Smart 216/232 IP SSH shell with the user name and password configured in the Smart 216/232 IP.

Restart the Smart 216/232 IP device after adding Telnet permissions to the users in order to enable login over SSH connection.

These settings are customizable, enabling you to choose the TCP port used for that purpose, if that port is already taken by another service on your network. You can operate the serial connection by using any SSH client, such as PuTTY and SecureCRT.

➔ **To configure the security settings:**

1. From the configuration menu, select **Security**.

   The Security page appears.

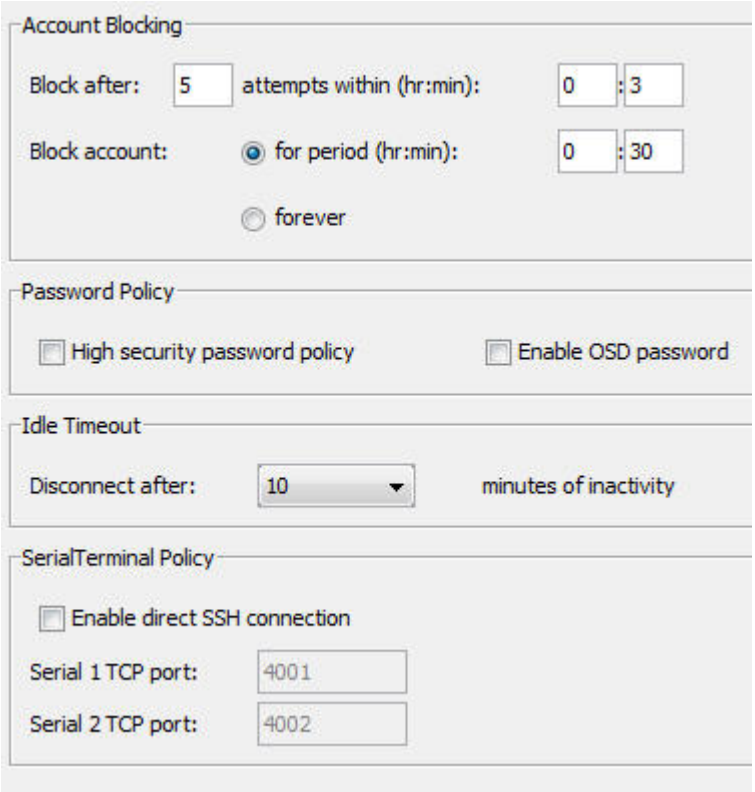


Figure 23 – Security Page

2. In the **Account Blocking** section:

   - In **Block after**, type the number of allowable attempts to log in with a wrong username or password in a time period specified in **attempts within**, prior to a forced time lock.
   - In **Block account**, select **for period** to block the account for a specified period of time, or **forever** for a total block.

3. Select the **High security password policy** checkbox to enable the high security password policy; clear the checkbox for the standard security policy to apply.
4. Select the **Enable OSD password** checkbox, to require a password for local user access to the OSD. By default, password is disabled.
5. In **Disconnect after**, select the timeout inactivity period after which the user is disconnected from the system. Select **No Timeout** to disable timeout.
6. To use your preferred SSH client to communicate directly to the serial device via the specified TCP ports:
    1. Select the **Enable direct SSH Connection** checkbox.
    2. Select **Serial 1 TCP port** and **Serial 2 TCP port** values. Their default ports are **4001** and **4002**, respectively.

3.9 Configuring User Targets

By default, administrators are allowed access to all servers. For other users, you must define the access rights of each user separately.

Perform the following procedure for each User.

➔ **To configure User targets:**

1. From the configuration menu, select **User Targets**.

    The User Targets page appears.

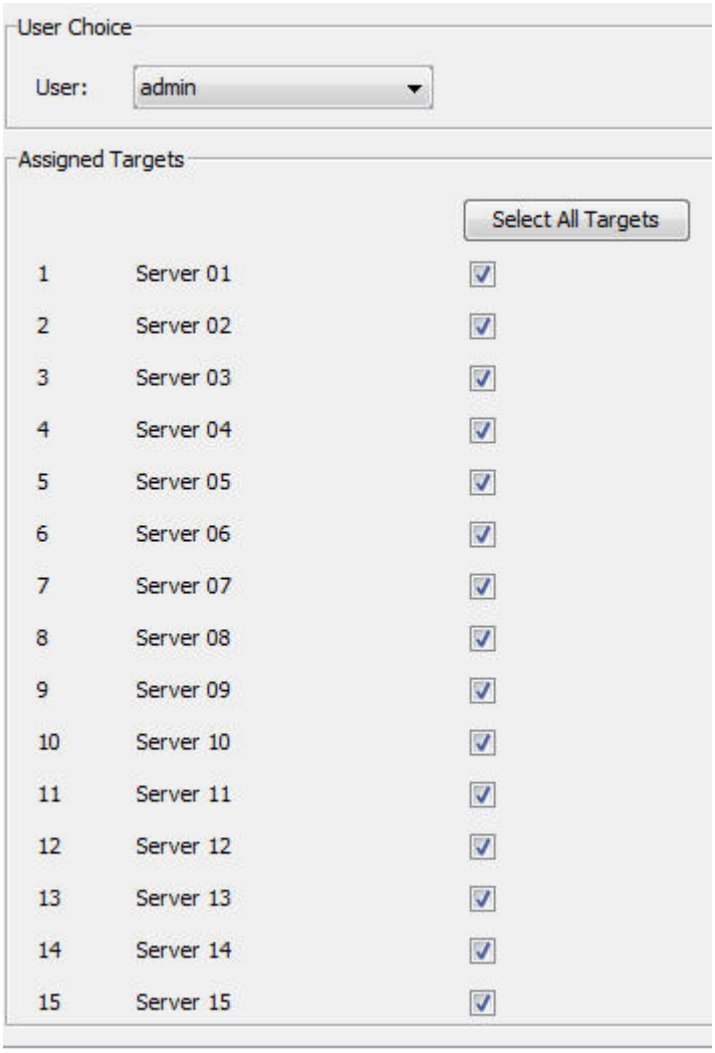


Figure 24 – User Targets Page

2. From the **User** dropdown menu, select a User.
3. Select the checkboxes of all the Target servers that the User can access (according to the User's access permissions).

   To select all Target servers, click **Select All Targets**.

3.10 Configuring the System Date and Time

This section describes how to configure the system date and time. The system time and date are used when recording log events (see Chapter 5).

➔ **To configure the date and time:**

1. From the configuration menu, select **Date & Time**.

   The Date and Time page appears.

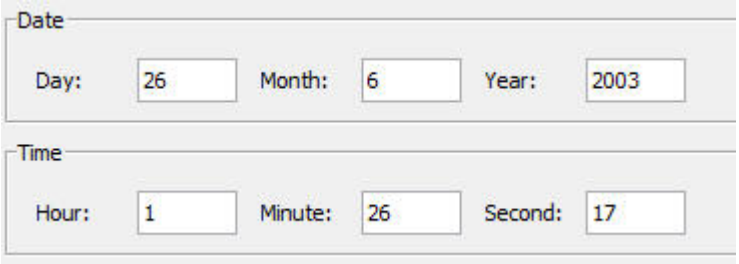


Figure 25 – Date and Time Page

2. In **Date**, type the current date: **Day**, **Month**, and **Year**.
3. In **Time**, type the current time: **Hour**, **Minute**, and **Second**.

3.11 Configuring Power Devices

This section describes how to configure the details of all power devices in the system. These details include the PDU (power device) name, type, and IP address.

➔ **To configure a power device:**

1. From the configuration menu, select **Power Devices**.

   The Power Devices page appears.

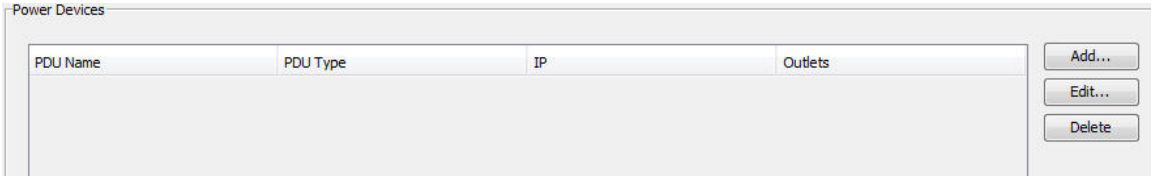


Figure 26 – Power Devices Page

2. Click the **Add** button.

   The Add PDU page opens.

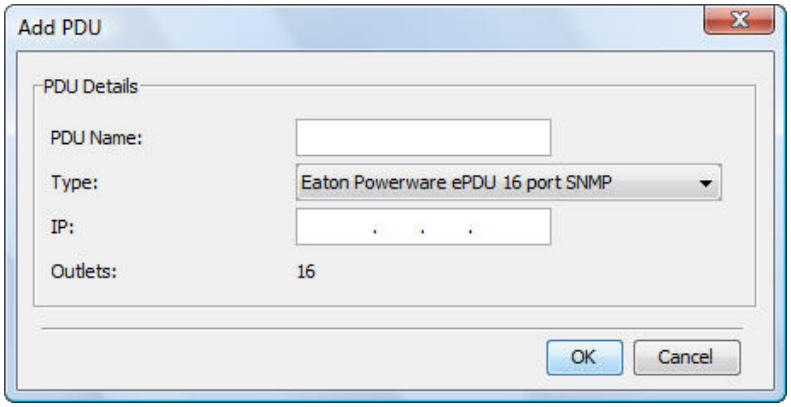


Figure 27 – Add PDU Page

3. In **PDU Name**, type a meaningful name for the PDU.
4. In **Type**, select the PDU type.

   The number of outlets in the device is displayed in **Outlets**.
5. In **IP**, type the IP address of the PDU.
6. Click **OK**.

   The PDU is added to the Power Devices page.

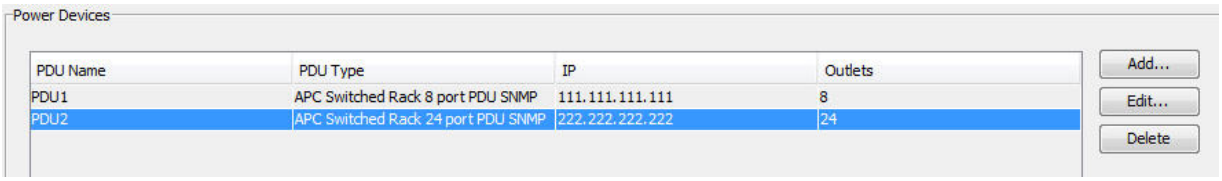


Figure 28 – Added Power Devices

3.11.1 Editing a Power Device

You can modify the information of any defined power device.

➔ **To modify power device details:**

1. In the Power Devices page, select a power device, and click the **Edit** button.

   The Edit PDU page appears.

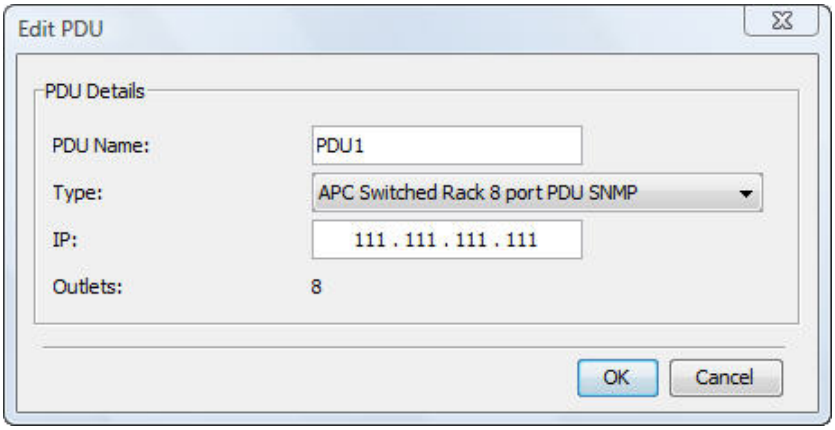


Figure 29 – Edit PDU Page

2. Select/type new values for the **PDU Name**, **Type**, and/or **IP** address, as required.
3. Click **OK**.

   The Power Devices page opens with the modified details.

3.11.2 Removing a Power Device

You can remove a power device that no longer exists in the system.

➔ **To delete a power device:**

1. In the Power Devices page, select a power device, and click the **Delete** button.

   The Delete PDU confirmation page appears.

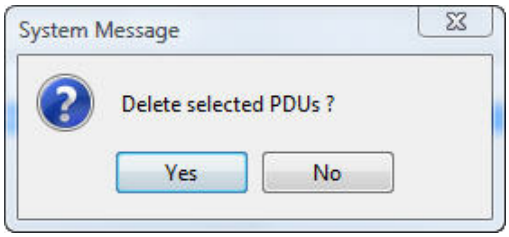


Figure 30 – Delete PDU Confirmation Page

2. Click **Yes**.

   The Power Devices page opens; the deleted PDU does not appear on the page.

3.12 Configuring Power Outlets

You must match a server to each power outlet of a power device defined in the system.

When you want to power manage the servers with double or more power supplies, you need to assign multiple outlets to the same KVM port.

Perform the following procedure for each power device defined in the system.

➔ **To configure the power outlets:**

1. From the configuration menu, select **Power Outlets**.

   The Power Outlets page appears.

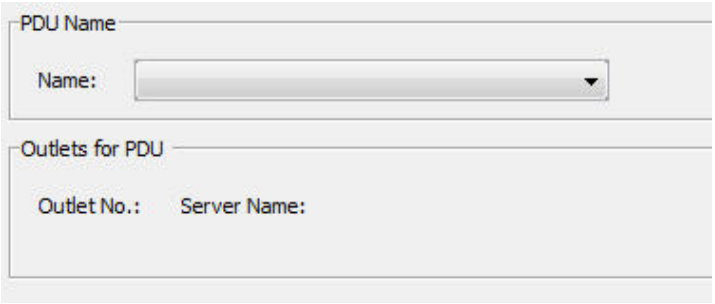


Figure 31 – Power Outlets Page

2. In **Name**, select the PDU for which you want to configure the power outlets.

   The number of outlets and Server Name dropdown menus corresponds to the type of the selected PDU.

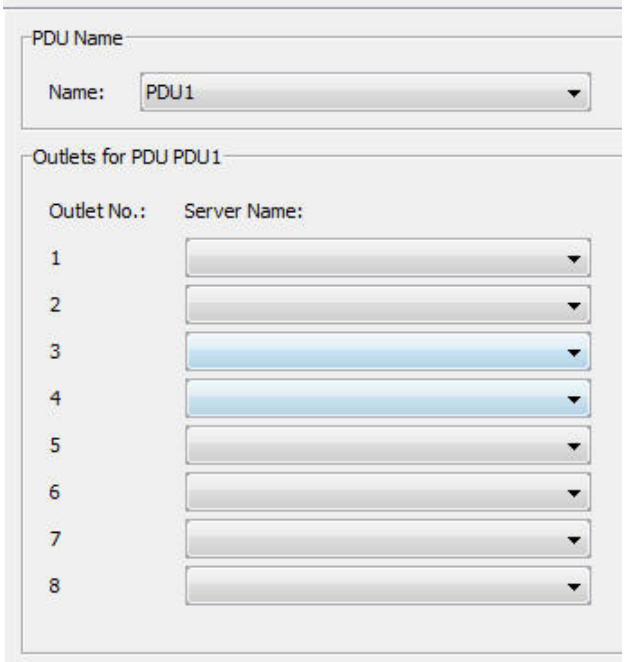


Figure 32 – Assigning Servers to Power Outlets Page

3. For each Outlet, select the **Server Name** from the dropdown list of the server connected to it.

3.13 Performing Additional Configuration Operations

You can perform the following additional operations on Smart 216/232 IP:

- Install an SSL certificate.
- Upgrade firmware.
- Upgrade RICCs/ROCs.
- Restore factory settings.
- Back up and restore data.

3.13.1 Installing an SSL Certificate

You can install an SSL Certificate, to ensure secure transactions between the Web servers and browsers.

➔ **To install an SSL Certificate:**

1. In the toolbar, select SSL Certificate.

   The SSL Certificate page appears.

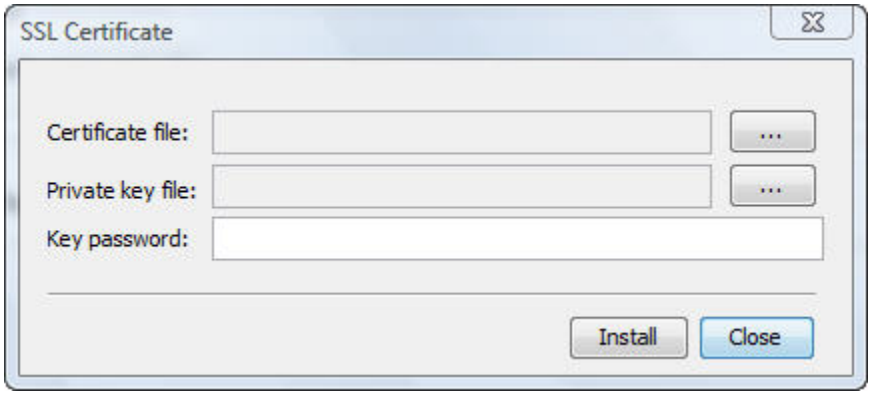


Figure 33 – SSL Certificate Page

2. In **Certificate file**, browse to locate the **Cer** file.
3. In **Private key file**, locate the **private key** file in Microsoft pvk format.
4. In **Key password**, type the password required to upload the Private Key file.

Each Private Key file is generated with a unique password.

5. Click **Install**.

   The SSL Certificate is installed.

6. Save the changes and restart the system, by clicking the Save button, and then the Device Reboot button.

3.13.2 Upgrading Firmware

You can upgrade the Smart 216/232 IP firmware to take advantage of new features.

➔ **To upgrade firmware:**

1. Download the firmware from Minicom's website at: http://www.minicom.com/phandlh.htm.
2. Save the firmware file on the client computer.
3. In the toolbar, select Device Upgrade.

   The Device Version Upgrade page appears, displaying the current firmware version on the device.

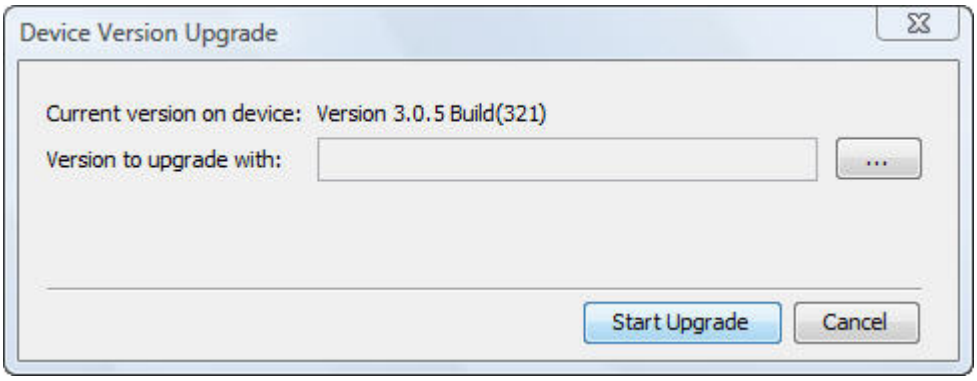


Figure 34 – Device Version Upgrade Page

4. In **Version to upgrade with**, browse to locate and upload the firmware file.
5. Verify the current and uploaded version of the firmware.
6. Click **Start Upgrade**.

   The upgrade starts.

7. On upgrade completion, on the toolbar, click Device Reboot.

   A confirmation box appears.

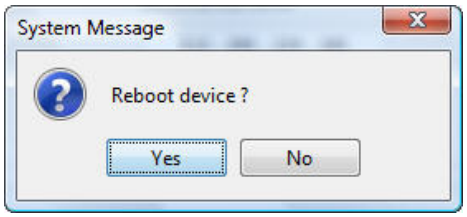


Figure 35 – Reboot Confirmation Page

8. Click **Yes**.

   The unit reboots. After about 30 seconds, the Login page appears.

Depending on the type of firmware upgrade, the following settings may be erased: User settings, KVM switch settings, mouse and video adjustments, and RS232 settings. The network settings remain intact. For more information, refer to the firmware release notes.

3.13.3 Upgrading RICCs/ROCs

You can upgrade the RICC/ROC firmware to take advantage of new features.

➔ **To upgrade firmware:**

1. Download the firmware from the Support section of Minicom's website at: http://www.minicom.com/.
2. Save the firmware file on the client computer.
3. In the toolbar, select RICCs/ROCs Upgrade.

   The RICCs/ROCs Upgrade page appears.

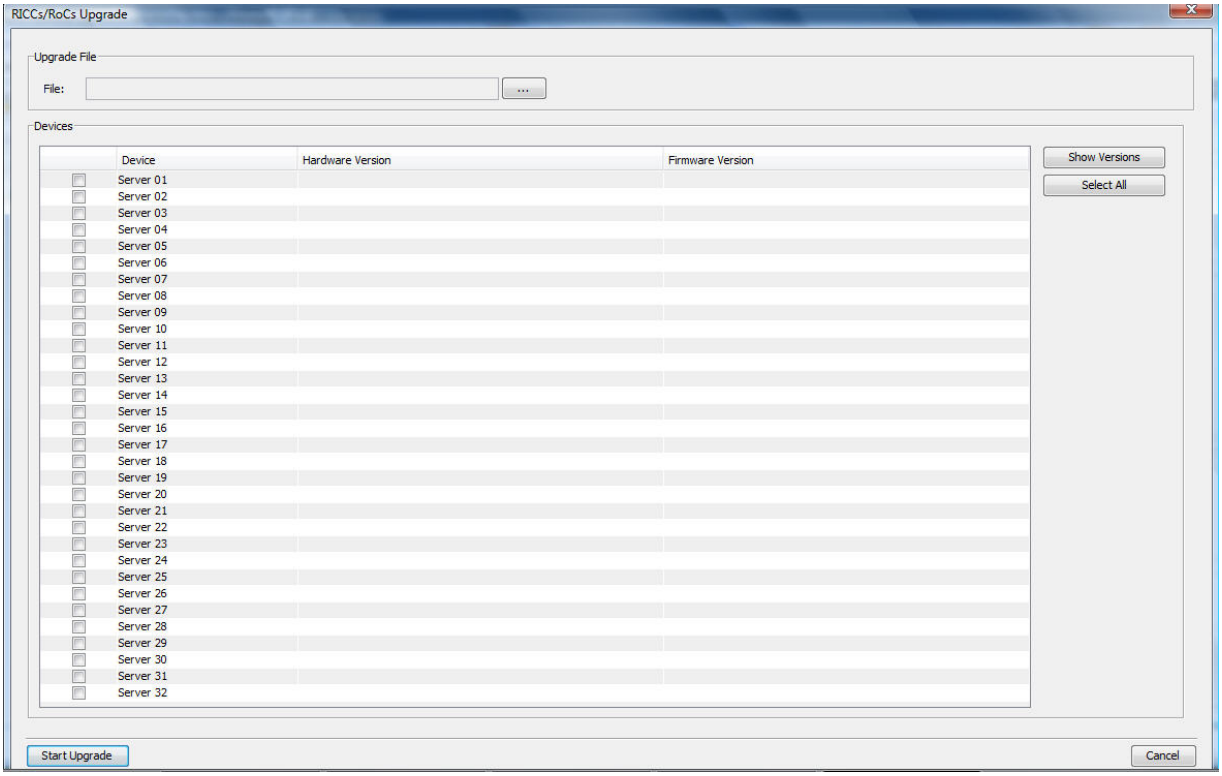


Figure 36 – RICCs/ROCs Upgrade Page

4. Select the checkboxes of the servers connected to the RICCs/ROCs that you want to upgrade. Click **Select All** to select all the servers.
5. Click **Show Versions** to verify the current hardware and firmware versions of the selected servers.
6. In **Upgrade File**, locate and select the firmware upgrade file.
7. Click the **Start Upgrade** button.

3.13.4 Restoring Factory Settings

You can restore the Smart 216/232 IP unit to its factory settings. This restores the original Smart 216/232 IP parameters, resetting all the information added by the administrators, including: Network settings*, Servers, Switches, Users, and Passwords.

- You have the option to preserve Network settings – as explained in the following procedure.

⚠ Once reset, the data cannot be retrieved.

➔ **To restore factory settings:**

1. In the toolbar, select Factory Restore.

   The Restore Factory Settings page appears.

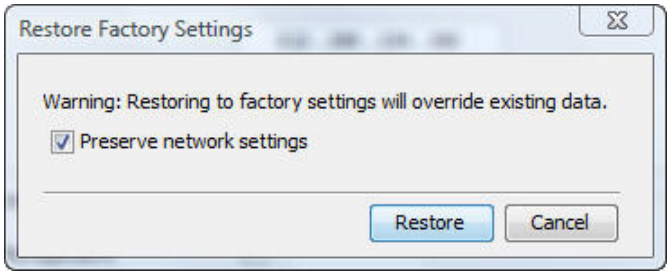


Figure 37 – Restore Factory Settings Page

2. To preserve network settings, select the **Preserve network settings** checkbox.
3. Click **Restore**.

   Factory settings are restored.

3.13.5 Backing Up and Restoring

You can backup all configuration data and restore it at a later date.

➔ **To back up data:**

1. In the toolbar, select Backup / Restore.

   The Backup/Restore Data page appears.

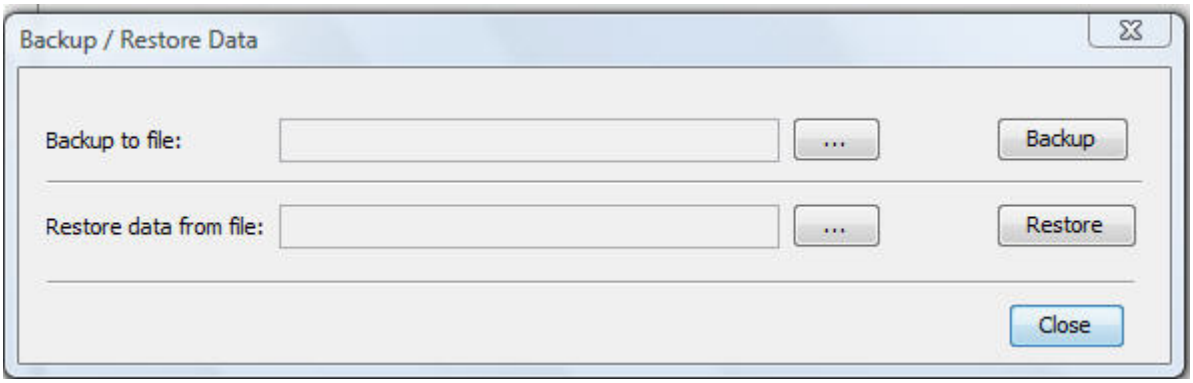


Figure 38 – Backup/Restore Data Page

2. In **Backup to file**, click the Browse button to locate and select the file on which to store the configuration data.
3. Click **Backup**.

   The configuration data is backed up.

4. Click **Close**.

➔ **To restore data:**

1. In the Backup/Restore Data page (see Figure 38), in **Restore data from file**, click the Browse button to locate and select the file which contains the data to restore.
2. Click **Restore**.

   The configuration data is restored.

3. Click **Close**.

3.14 Reloading a Page

You can load the parameters on any configuration page with the settings from the Smart 216/232 IP device. This is convenient if you have already changed settings on the page, and want to restore the device settings.

➔ **To reload a page:**

1. In the Configuration page toolbar, click the Reload button.

   The parameters are populated with the device settings.

3.15 Saving Changes and Logging Out

Once you have completed configuration changes, you must save them.

Changes to the SSL Certificate and Security pages require saving and restarting.

Saving the configuration changes after changing the Device page restarts the unit automatically.

➔ **To save changes:**

1. In the Configuration page toolbar, click the Save button.

   If you made changes to the Device page, the system automatically prompts you to reboot and restart the device, by displaying the following device reboot confirmation box:

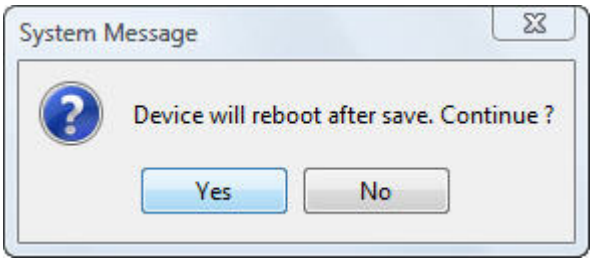


Figure 39 – Device Reboot Confirmation Message

3. Click **Yes**.

   A message box informs that Save has completed.

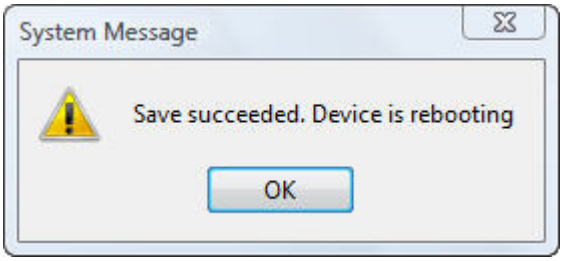


Figure 40 – Save Succeeded Message

4. Click **OK**.

   Device reboots, and when it completes a Logon page appears.

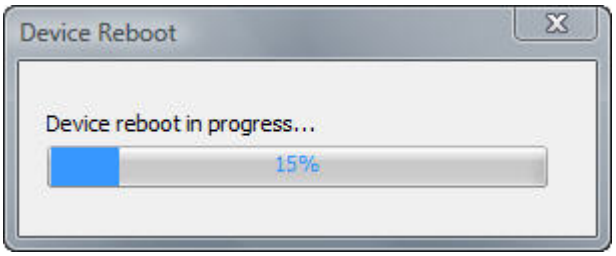


Figure 41 – Device Rebooting Progress Box

Figure 42 – Logon Page after Rebooting

5. Type your **User** name and **Password** and click **Enter**.

   The Configuration page opens.

➔ **To log off:**

1. In the screen toolbar, click the Log On/Off button.

   The Configuration screen is closed, and the session closes.

4 Conducting a Remote Session

A remote session enables remotely accessing any of the target servers connected to Smart 216/232 IP. Before starting a remote session, Smart 216/232 IP must be fully configured.

You can perform the following from the remote session:

- Display/hide the toolbar.
- Set the session profile.
- Display the session in full screen mode.
- Verify Remote Presence Solutions information.
- Adjust video settings.
- Power manage the target servers.
- Manage keyboard sequences.
- Synchronize mouse pointers.
- Switch to a different server or device.

4.1 Starting a Remote Session

You can start a remote session by:

- Logging into the system, as explained in steps 1 to 5 of the procedure in Section 3.2
- Selecting the target that you want to connect to
- Displaying the target inside a remote console window

➔ **To start a remote session:**

1. Log into the Smart 216/232 IP system, by following steps 1 to 5 of the procedure in Section 3.2.

   The Targets screen appears. Only targets that the User is permitted to use, appear on the page. As an Administrator can access all connected targets, they all appear on the Targets page, as in the following figure.

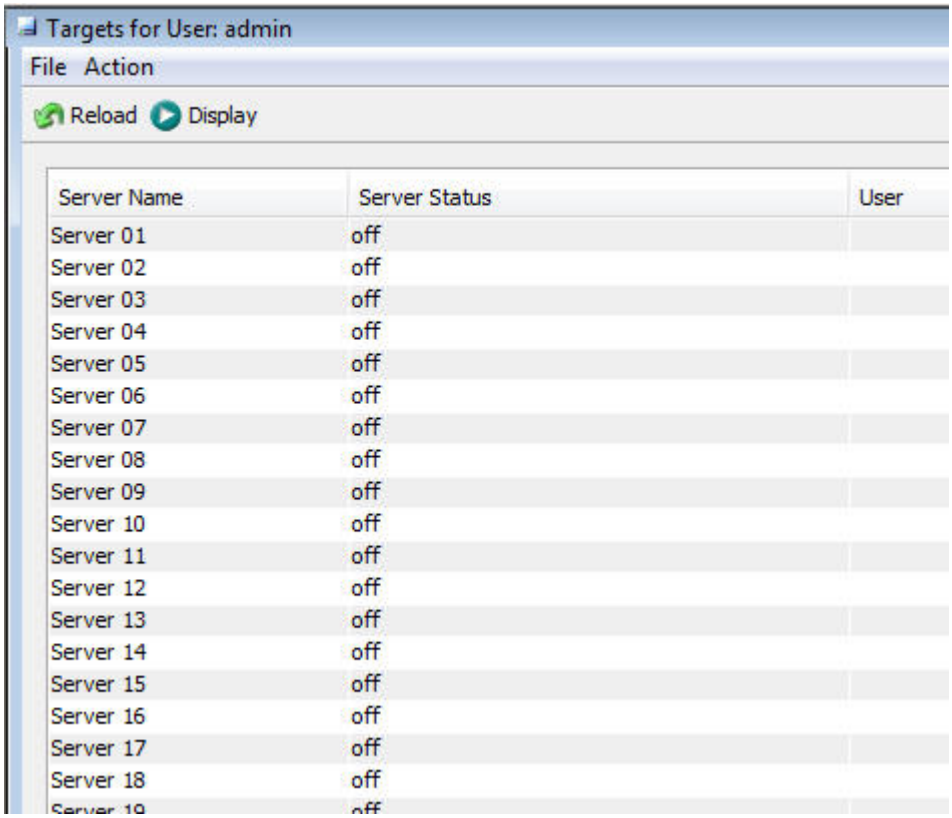


Figure 43 – Server Targets

The following table describes the Targets page parameters and buttons.

Parameter/Button	Description
Server Name	The server name. The server name can be changed in the Configuration settings to give the server an identifiable name (see Section 3.6).
Server Status	The status of the server. It can be **available**, **off**, **busy** (meaning that another user is accessing the server), or **Remote Active Session**.
User	The current user (if any) accessing the target server.
Reload	Pressing this button reloads the page. Can also be accessed from the **Action** dropdown menu.
Display	Pressing this button starts a remote session for the selected target server. Can also be accessed from the **Action** dropdown menu.

2. In the **Server Name** column, select the target server that you want to connect to, by highlighting it and clicking Display, or by double-clicking it.

A server being used by another user cannot be accessed.

The screen of the selected target server that is connected directly to Smart 216/232 IP, appears inside a remote console window with the remote session toolbar.

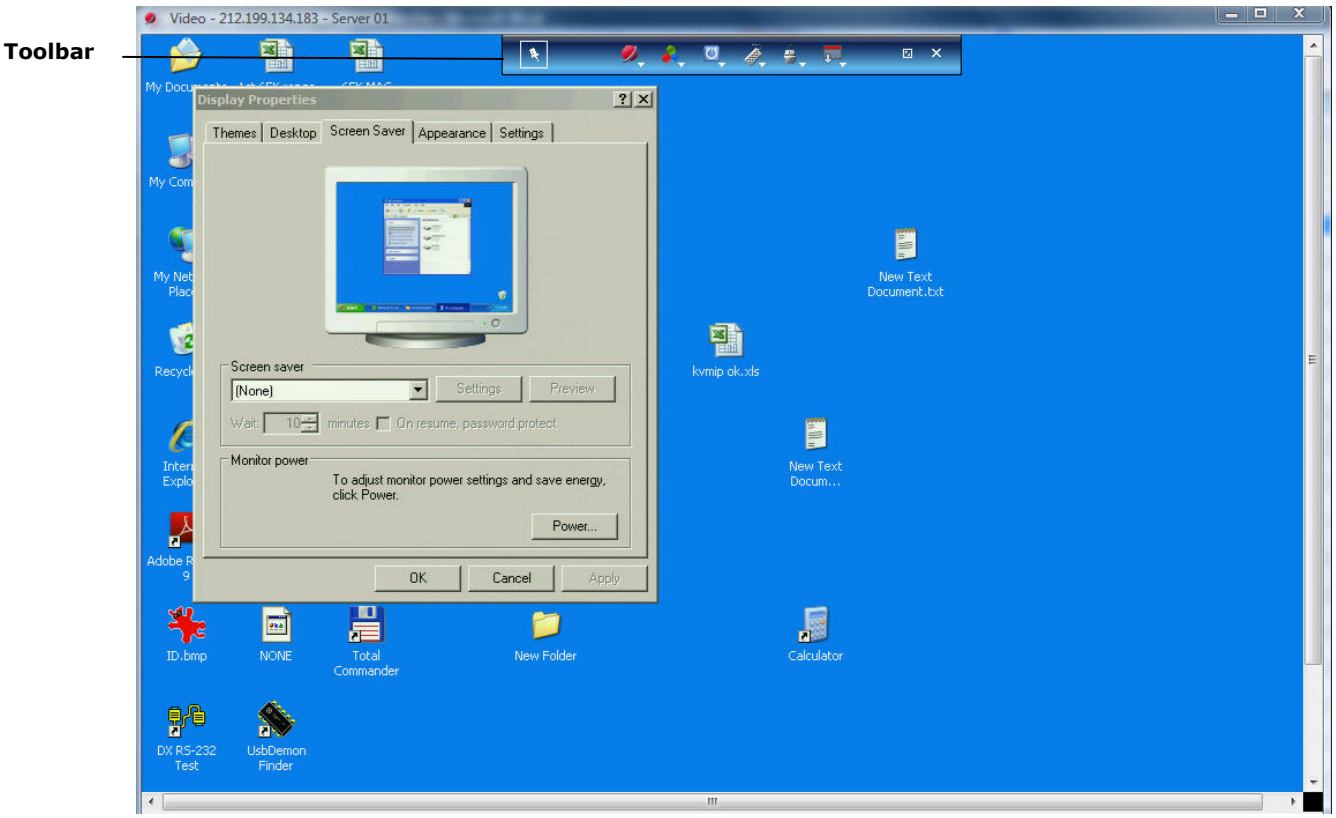


Figure 44 – Remote Session Page

Also, the **Server Status** of the server becomes **Remote Active Session**.

4.1.1 Remote Session Toolbar Buttons

The following table describes the functionality of the Remote Session toolbar buttons.

Button	Description
	Toggle button for displaying/hiding toolbar.
	Session button. Pressing this button opens up a dropdown menu for selecting: **Session Profile** – enables configuring remote session profile session **About** – displays client, firmware, Switch File, and KME version information

Button	Description
	Video button. Pressing this button opens up a dropdown menu for performing: **Refresh** – for refreshing the video image **Video Adjust** – for automatically adjusting the video image **Advanced** – for manually setting video settings **Performance** – changing video performance by changing mode and/or bandwidth
	Keys button. Pressing this button opens up a dropdown menu with predefined key sequence names and **Special Keys** item which enables you to: add a keyboard sequence, record a new custom key, edit an existing key sequence, and delete a key sequence
	Mouse button. Pressing this button opens up a dropdown menu for performing: **Calibrate** – calibrates the speeds of the mouse pointers of the target server and client computer in Win98, NT or 2000 **Align** – for aligning the local mouse pointer with the remote target server mouse pointer **Mouse Settings** – for manually synchronizing the mouse pointers
	Server/Serial button. Pressing this button displays the connected servers and serial devices. You can switch to a different server/device.
	Restore button. To toggle Full screen mode on and off.
	Logoff button. Closes the current remote session and displays the logon Web page.

4.2 Sharing a Remote Session

Users who want to remotely work on a server at the same time and collaborate their work, can share a remote session. All users in the remote session can connect to see the video at the same time and share the Keyboard/Mouse control. Up to five users can share the same remote session.

When connecting to a target server that other users are already connected to, the following message appears:

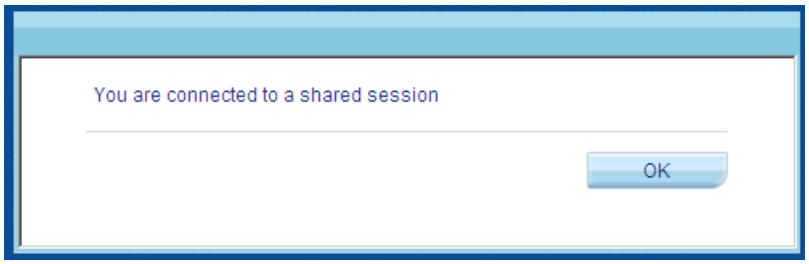


Figure 45 – Shared Remote Session

4.2.1 Exclusive Session

When starting a remote session and there are no other logged in users, a user can prevent other users from connecting to the session (see Section 4.4, step 4). This means that the user is the only one who can see the video and control the Keyboard/Mouse, enabling the user to work on the server without anyone seeing or interfering in the user's work.

4.3 Displaying the Toolbar

The Toolbar appears briefly at the top of the screen (see Figure 44). It disappears when the mouse is not over it. To make it reappear, glide the mouse over the top of the screen. To display the toolbar permanently, click the tack icon on the toolbar.

4.4 Setting the Session Profile

You can set the remote session display features, as follows:

- Select the format of the mouse pointer, or hide it.
- Hide the toolbar.
- Display the session in full screen mode – You can work on the target server as if you are working on a local computer, using full screen mode. In Full Screen mode, the desktop window disappears, and is replaced by the accessed target server desktop.
- Prevent other users from logging into the same session.

➔ **To set the session profile:**

1. On the toolbar, select **> Session Profile**.

   The Session Profile window appears.

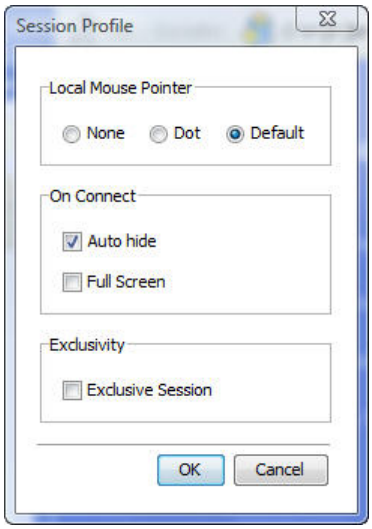


Figure 46 – Session Profile Dialog Box

2. In **Local Mouse Pointer**, select one of the following options to set the appearance of the client computer mouse pointer:
   - **None** – to hide the mouse pointer
   - **Dot** – for the mouse pointer to appear as a dot
   - **Default** – for the mouse pointer to appear as a regular-shaped mouse cursor
3. In **Auto Connect**, select:
   - **Auto hide** – to hide the toolbar from the next connection onwards
   - **Full Screen** – to display the remote session screen in full screen mode from the next connection onwards. To toggle full screen mode on and off, you can click the Restore button (see Section 4.4.1).
4. In **Exclusivity**, select the **Exclusive Session** checkbox when starting a remote session and there are no other logged in users; this prevents other users from logging into the session.

4.4.1 Full Screen Mode

You can work on the target server as if you are working on a local computer, using full screen mode. In Full Screen mode, the desktop window disappears, and is replaced by the accessed target server desktop.

➔ **To work in full screen mode:**

1. Ensure that the client computer has the same screen resolution as the target server.
2. On the toolbar, click the Restore button .

The desktop window disappears.

➔ **To exit full screen mode:**

1. On the toolbar, click the Restore button .

   The desktop window appears.

Full screen mode can also be activated from the Session Profile box, see Section 4.4, step 3.

4.5 Verifying Remote Presence Solutions Information

You can verify the client, firmware, KME (Keyboard/Mouse Emulation firmware), and Switch file versions installed on your Smart 216/232 IP. This information can assist system administrators in troubleshooting and support.

➔ **To verify Remote Presence Solutions information:**

1. On the toolbar, select **> About**.

   The information screen appears.

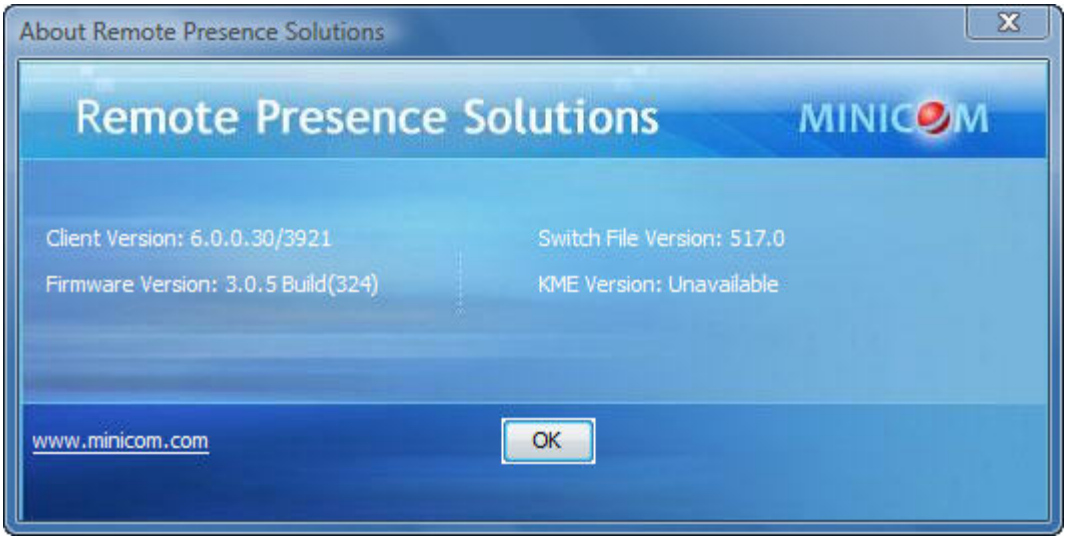


Figure 47 – Remote Presence Solutions Information

4.6 Changing the Video Performance Settings

From the toolbar, you can alter the video performance settings, by selecting a different mode or bandwidth.

The mode can be set to:

- **Fixed** – Enables you to select any bandwidth option. For example, in a LAN environment, it is best to set the bandwidth setting to **High**. For VPN and Internet environments, you may want to alter the settings to increase responsiveness.
- **Adaptive** – Automatically adapts to the best compression and colors according to the network conditions.

You can choose to display more colors for more fidelity, or less colors to reduce the volume of data transferred through the network. Choosing more colors requires more bandwidth.

The bandwidth can be set to:

- **Maximum** – For optimal performance when working on a LAN. This gives no compression and high color (16 bit)
- **High** – For low compression and high color (16 bit)
- **Medium** – For medium compression and either high color or 256 colors; Recommended when using a standard Internet connection
- **Low** – For high compression and 16 colors

➔ **To alter the settings:**

1. On the toolbar, select **> Performance**.

   The Performance dialog box appears.

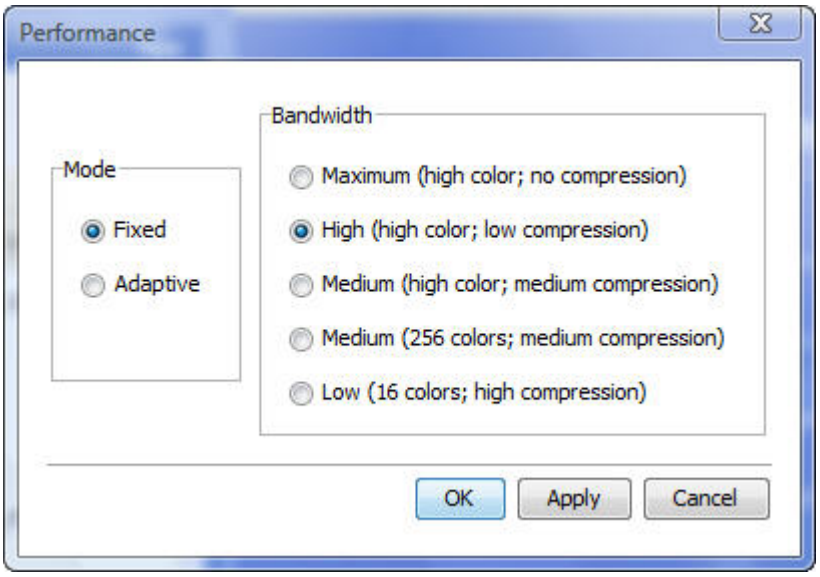


Figure 48 – Performance Settings

2. In **Mode**, select **Fixed** or **Adaptive**.
3. For **Fixed** mode, in **Bandwidth**, select **Maximum**, **High**, **Medium** (high color or 256 colors), or **Low**.
4. Click **OK**.

   The chosen setting takes effect and the screen of the last accessed target server appears.

4.7 Adjusting the Video

There are three ways to adjust the video image:

- Refreshing the video image
- Automatically adjusting the video image
- Manually changing advanced video settings

4.7.1 Refreshing the Video Image

The video image may require refreshing when changing the display attributes of a target server. Refreshing completely regenerates the video image.

➔ **To refresh the video image:**

1. On the toolbar, select **> Refresh**.

   The image is refreshed.

4.7.2 Automatically Adjusting the Video Image

The video view may need to be adjusted for each target server or new screen resolution. In most cases, adjusting the video view using the default video settings gives the optimal view.

➔ **To automatically adjust the video image:**

1. On the toolbar, select **> Video Adjust**.

   The progress of video adjustment is displayed.

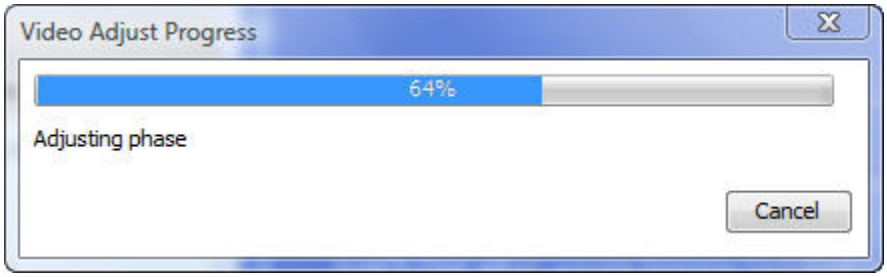


Figure 49 – Video Adjust Progress

   The process takes a few seconds. If the process runs more than a few times, it is an indication that there is an abnormal noise level. Check the video cable and verify that no dynamic video application is running on the target server's desktop.

4.7.3 Manually Adjusting Video Settings

Although automatic adjustment of video generally optimizes the video view, you may want to fine-tune the results.

You can use the advanced video adjustment options:

- To fine-tune the target server video settings after auto adjustment
- To adapt to a noisy environment or a nonstandard VGA signal
- When in full-screen DOS/CLI mode

After adjusting the video settings manually, you can always revert to automatically adjusting the video settings, as explained in Section 4.7.2.

➔ **To manually adjust the video settings:**

1. On the toolbar, select **> Advanced**.

   The manual controls appear.

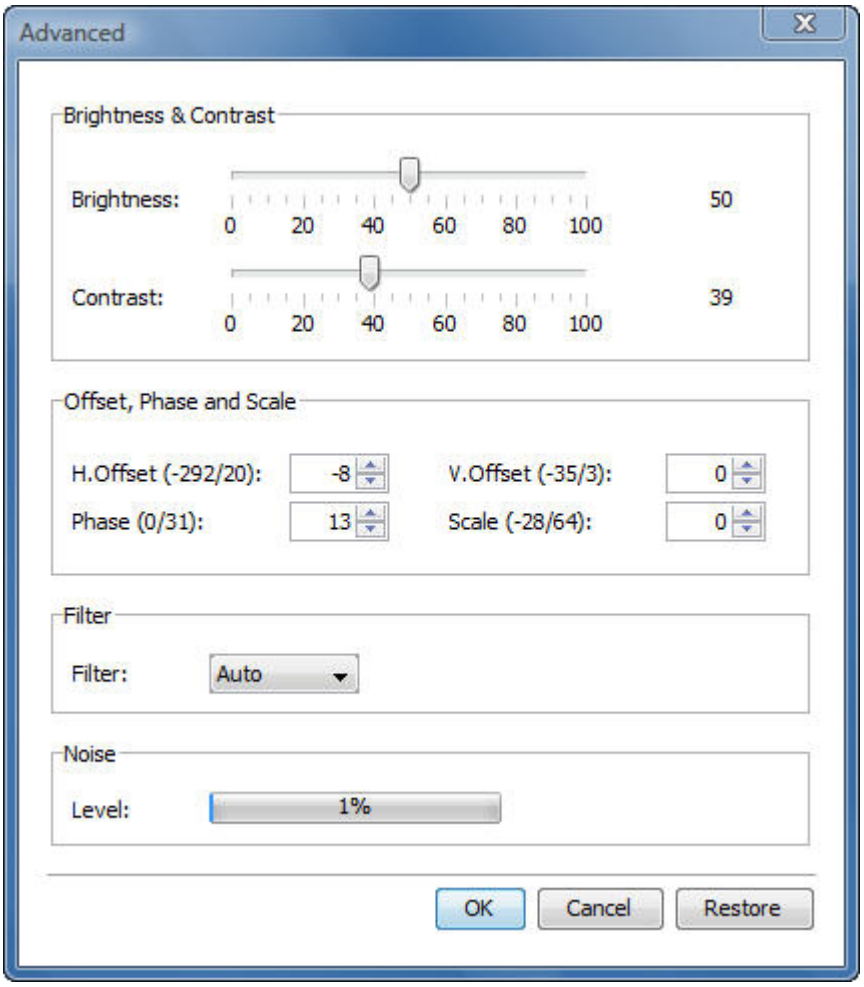


Figure 50 – Manual Video Adjustments Controls

2. In **Brightness** and **Contrast**, use the scales to adjust the brightness and contrast of the displayed image, respectively. Move the sliders to change the displayed image. Click in the area of the sliders for fine-tuning.
3. In the **Offset, Phase and Scale** section:
   - In **H. Offset**, select the starting position of each line on the displayed image.
   - In **V. Offset**, select the vertical starting position of the displayed image.
   - In **Phase**, select the point at which each pixel is sampled.
   - In **Scale**, select the scale resolution of the session image.

   Adjust **Phase** and **Scale** to reduce the noise level to a minimum.
4. In **Filter**, select the filter of the input video from the server. A higher filter reduces the noise level but makes the image heavier. Options are: **Auto**, **No Filter**, **Low**, **Medium**, and **High**.

5. **Level** displays the Video "noise" level when a static screen is displayed.
6. Click **OK**.

4.8 Power Managing the Target Servers

When a Minicom Remote Power switch or POC is connected to the Serial port of the Smart 216/232 IP unit, you can power manage the target servers via the Power menu.

➔ **To power manage the target servers:**

1. On the toolbar, click .

   The Power menu appears.

Figure 51 – Power Menu

2. Select one of the following options:
   - **Power Cycle** – to send a power cycle to the currently accessed target server, meaning that the target server is first powered down and then powered up
   - **Power Up** – to power up the currently accessed target server
   - **Power Down** – to power down the currently accessed target server

Only the currently accessed target server is affected. Therefore, to power manage other target servers, you must access each one individually.

4.9 Managing Keyboard Sequences

You can select any keyboard sequence (a combination of keys that performs a specific process) that appears in the dropdown menu of the toolbar button to send it to the target server to initiate its associated process. For example, selecting **Ctrl-Alt-Del** sends this three-key sequence to the target server to initiate its Shutdown/Login process.

When clicked, these key sequences transmit directly to the target server, and do not affect the client computer.

This section describes how to:

- Add predefined keyboard sequences to the list of keyboard sequences
- Create customized keyboard sequences
- Edit existing keyboard sequences
- Delete existing keyboard sequences

4.9.1 Adding a Keyboard Sequence

You can add predefined keyboard sequences to the list of keyboard sequences that can be accessed directly from the dropdown list of the toolbar item .

➔ **To add a keyboard sequence:**

1. On the toolbar, click **> Special Keys.**

   The Special Key Manager box appears.

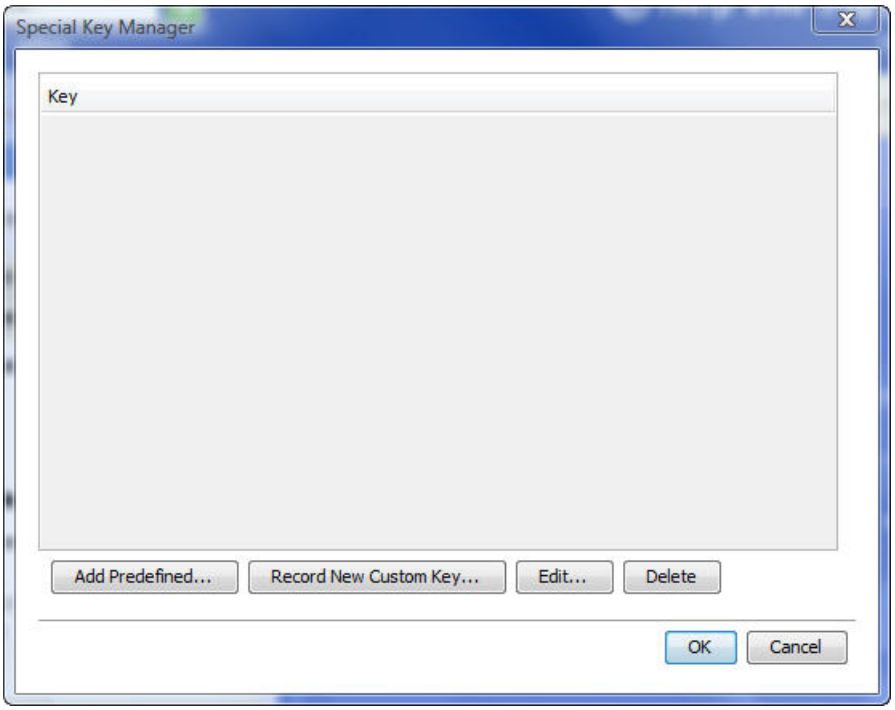


Figure 52 – Special Key Manager

2. Click the **Add Predefined** button.

   A list of existing sequences appears.

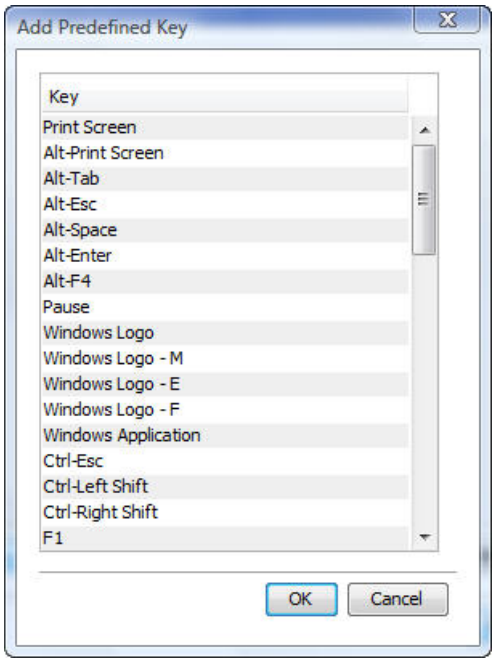


Figure 53 – Add a Predefined Key Dialog Box

3. Select a key sequence and click **OK**.

   The sequence appears in the Special Key Manager box.

4. In the Special Key Manager box, click **OK**.

   The sequence appears in the Keyboard Key sequence list.

4.9.2 Recording a New Custom Key

This section describes how to define a new keyboard sequence. After defining the keyboard sequence, you can add it to the list of keyboard sequences that can be accessed directly from the dropdown list of the toolbar item (see Section 4.9.1).

➔ **To record a keyboard sequence:**

1. In the Special Key Manager box (see Figure 52), click **Record New Custom Key**.

   The Record Macro box appears.

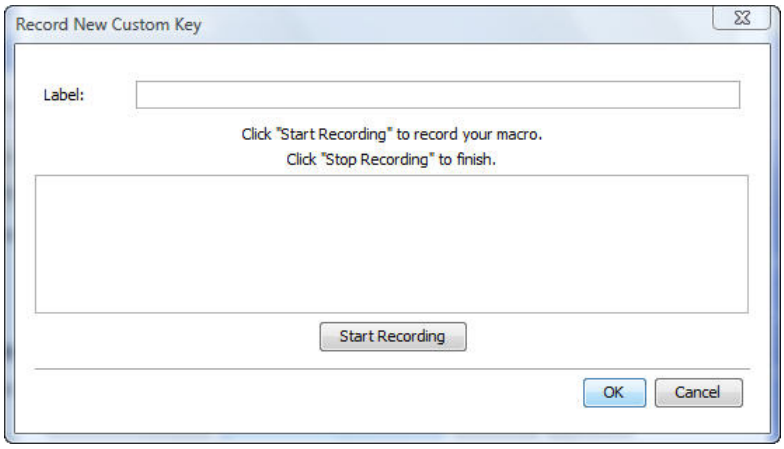


Figure 54 – Record Macro Box

2. In **Label**, type a name for the new key sequence.
3. Click **Start Recording**.
4. On your keyboard, press the keys to include in the key sequence.

   The names of the pressed keys appear in the provided area.
5. Click **Stop Recording**.
6. Click **OK**.

   The new key sequence is now on the list of predefined key sequences.

4.9.3 Editing a Key Sequence

➔ **To edit a predefined keyboard sequence:**

1. In the Special Key Manager box (see Figure 52), select the desired key sequence and click **Edit**.

   The Record Macro box appears (see Figure 54). The name of the key sequence to edit appears in the **Label** field.
2. Click **Start Recording**.
3. On your keyboard, press the keys to include in the key sequence.

   The names of the pressed keys appear in the provided area.
4. Click **Stop Recording**.
5. Click **OK**.

   The key sequence definition is updated in the system.

4.9.4 Deleting Key Sequence(s)

You can delete a single or multiple key sequences from the system.

➔ **To delete a keyboard sequence:**

1. In the Special Key Manager box (see Figure 52), select the desired key sequence(s) to delete. Select a group of keys by selecting the first key in the group, pressing the **Shift** button, and then selecting the last key.
2. Click **Delete**.

   The delete confirmation box appears.

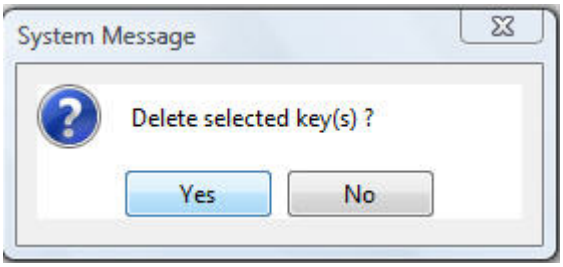


Figure 55 – Delete Key(s) Confirmation Box

4.10 Synchronizing Mouse Pointers

For best mouse performance and superior customer experience, Minicom recommends that you set certain mouse settings in the target operating system. This applies to all targets running Windows, such as XP, Windows 7, Windows Server 2003, and Windows Server 2008.

When working at the client computer, two mouse pointers appear – one of the client computer and one of the target server; the former is on top of the latter. The mouse pointers should be synchronized. The following explains what to do if they are not synchronized.

Before synchronizing mouse pointers, adjust the video of the target server (see Section 4.7); otherwise, mouse synchronization may not work.

The **Align** and **Calibrate** options are available from the **Mouse** menu, only for **Relative Mouse Position** mode.

4.10.1 Manually Synchronizing the Mouse

If the mouse settings on the target server have been changed, or when the operating system on the target server is Windows XP / 2003 Server / 7 / 2008 Server, Linux, Novell, SCO UNIX, or SUN Solaris, you must synchronize the mouse pointers manually.

➔ **To manually synchronize mouse pointers:**

1. On the toolbar, select **> Mouse Settings**.

   The Mouse Settings box appears.

   For **SMART 216/232 IP PS/2** devices, the default mode is **Relative Mouse Position** (see Figure 56); for **SMART 216/232 IP USB** devices, the default mode is **Absolute Mouse Position** (see Figure 57)

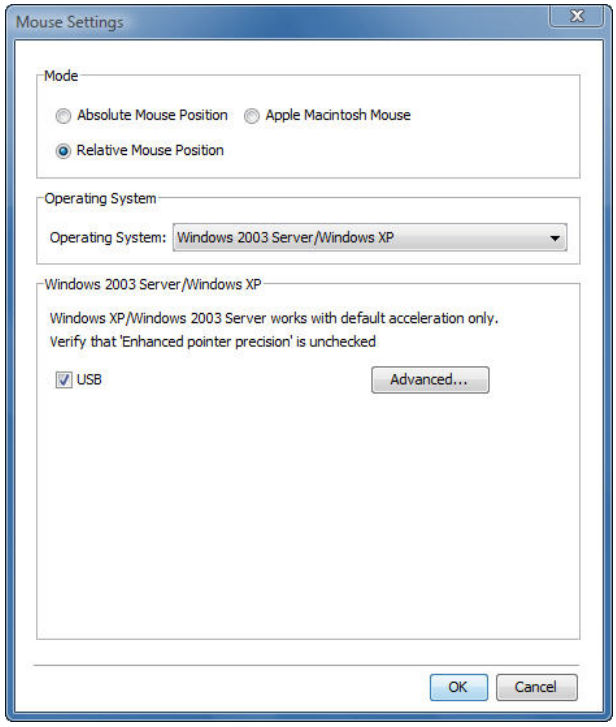


Figure 56 – Relative Mouse Settings

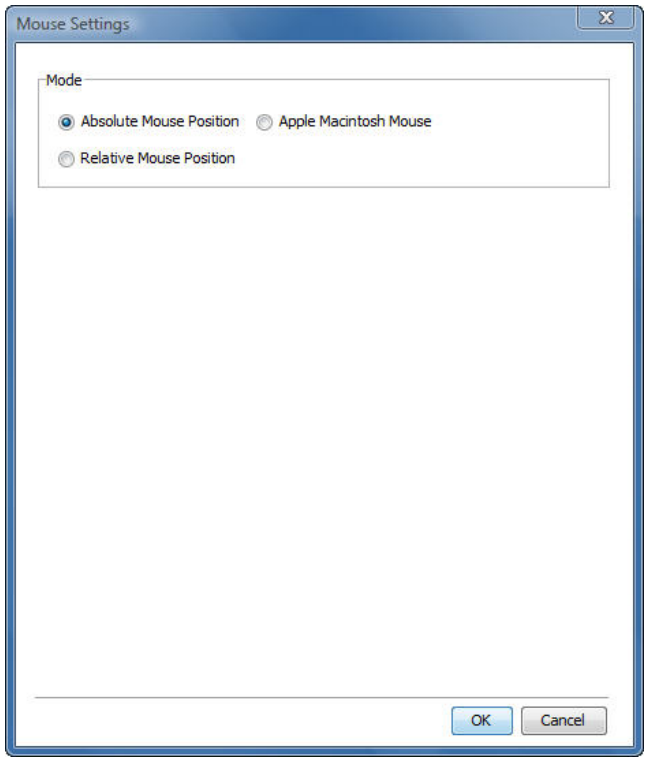


Figure 57 – Absolute Mouse Settings

Selecting the Mouse Mode

On the Mouse Settings page, there are three selectable modes:

- Absolute Mouse Position
- Apple Macintosh Mouse
- Relative Mouse Position

The mouse mode that you can select depends on the type of SMART 216/232 IP device and on the target operating system / computer:

- For **SMART 216/232 IP USB** devices:
  - If the operating system on the Target is Windows ME or later, select **Absolute Mouse Position** mode (see Figure 57); this is the default mode for SMART 216/232 IP USB devices.
  - If the operating system on the target is Windows 98 or Linux, Novell, UNIX or SUN, select **Relative Mouse Position** mode.
  - If the target is a MAC computer, select **Apple Macintosh Mouse** mode.

- For **SMART 216/232 IP PS/2** devices: **Relative Mouse Position** is the only possible mode.

Relative Mouse Position Mode

Selecting **Relative Mouse Position** mode enables you to configure mouse settings, set the USB option (see The USB Option), and advanced settings (see Advanced Mouse Emulation).

➔ **To configure settings for the Relative Mouse Position mode:**

1. In **Operating System**, from the dropdown menu, select the target's operating system.

   Instructions and sliders appear.

2. Follow the instructions and set any relevant sliders to the same values as set in the target's Mouse Properties window.
3. Click **OK**.

   The mouse pointers are synchronized.

Examples

The following are examples of the instructions for two different target operating systems. After performing the instructions for the selected operating system, you should click **OK** to synchronize the mouse pointers.

1. For **Windows 7**: Go to the Mouse Properties on the Target and clear the **Enhance pointer precision** checkbox.

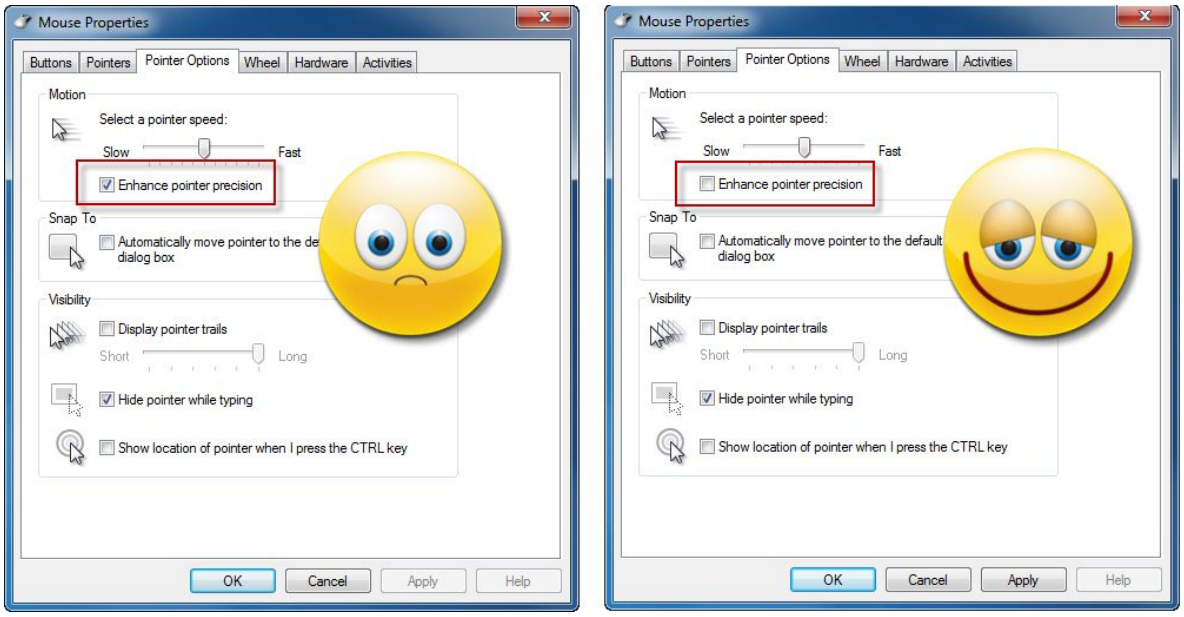


Figure 58 – Windows 7 Mouse Properties

2. For **Windows 2000**: If Mouse Properties were ever changed for the target – even if they have been returned to their original state – clear the **Default** checkbox
   ☑ Default .

The USB Option

You can use the **USB** option if you have USB to PS2 conversion between SMART 216/232 IP and the target server via any of the following:

- USB-to-PS/2 adapter
- Unsupported operating systems
- SUN Solaris

Use this option if you are sure of the custom acceleration algorithm you are using, or have been informed to do so by customer support.

Advanced Mouse Emulation

In the Advanced Mouse settings, you can set the type of mouse that you would like SMART 216/232 IP to emulate. It is recommended not to change the advanced settings unless there is erratic mouse behavior (for example, the mouse is making random clicks and jumping arbitrarily around the screen).

➔ **To set the type of mouse that you want SMART 216/232 IP to emulate:**

1. In the **Mouse Settings box** (see Figure 57), click **Advanced**.

   The Mouse Emulation box appears.

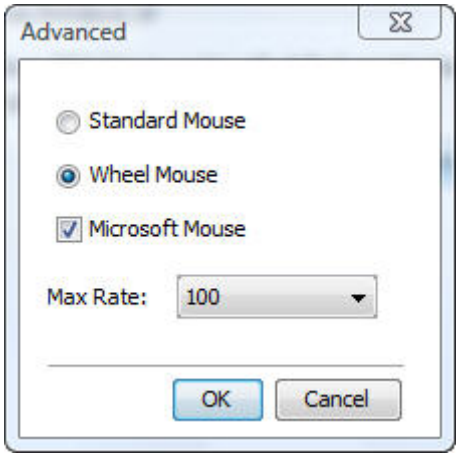


Figure 59 – Mouse Emulation Box

2. Select the mouse connected to the Local Console port on the SMART 216/232 IP, as follows:

- **Standard Mouse** – if the local mouse is a non-Microsoft two-button mouse; in this case, clear the **Microsoft Mouse** checkbox.
- **Wheel Mouse** – Microsoft mouse or Microsoft optical mouse

3. In **Max Rate**, select the maximum mouse report rate.

   For Sun Solaris the default value is 20 in order to support older Sun versions.

4. Click **OK**.

4.10.2 Aligning the Mouse Pointers

When accessing the target server, the mouse pointers may appear at a distance to each other, due to the mouse on SMART 216/232 IP losing sync with the mouse on the host system. You can align the local mouse pointer with the remote target device's mouse pointer.

➔ **To align the mouse pointers:**

1. On the toolbar, select **> Align** (or press **Ctrl+M**).

   The mouse pointers align.

4.10.3 Calibrating Mouse Pointers

A target server may have a different mouse pointer speed than the client computer. Calibrating automatically discovers the mouse speed of the target server and aligns the two pointers.

You can perform automatic calibration when the target server operating system is Windows NT4, 2000, or 98.

SMART 216/232 IP saves this alignment so that calibration is only needed once per target server.

➔ **To perform the calibration:**

1. On the toolbar, select **> Calibrate**.

If the Video Noise Level is above zero, calibration may not work. In this case, go to Video Adjustment and try to eliminate the noise by automatically adjusting the video (see Section 4.7.2) and/or adjusting the bars in manual video adjust (see Section 4.7.3), and then performing the mouse calibration.

If the mouse settings on the target server have been changed, you must synchronize mouse pointers manually, as explained below.

4.11 Switching to a Different Server/Device

In the middle of a remote session, you can switch to a different server or device.

➔ **To connect to a different server or device:**

1. On the toolbar, click .

   A list of connected servers/devices appears. There is a checkmark near the server/device of the remote session.

2. Click the desired server or Serial device.

   The screen of the server or Serial device terminal emulation window appears.

4.12 Disconnecting the Remote Session

➔ **To disconnect the session:**

1. On the toolbar, click .

   The Login Web page appears. You can re-login or close the browser window.

5 Managing the Events Log

This chapter describes how to manage the Events log, including:

- Viewing the Events log
- Reloading the Events log
- Clearing the Events log
- Saving the Events log

5.1 Viewing the Events Log

You can view a log of all system events.

➔ **To view the Events Log:**

1. In the menu in the left pane, click Events.

   The log of all system events is displayed.

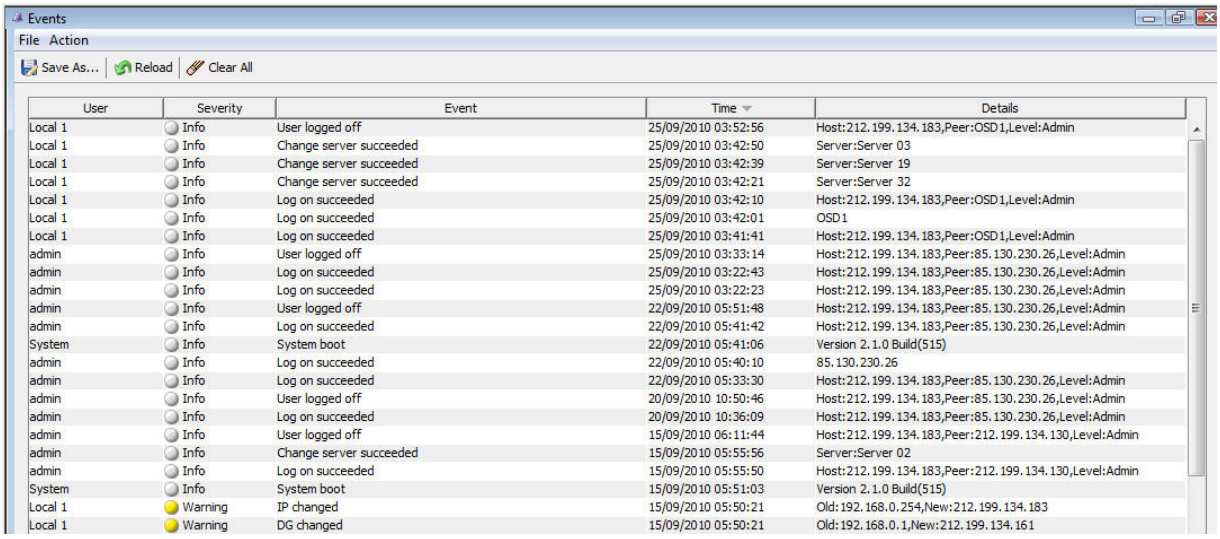

Events
File Action
Save As...
Reload
Clear All
User
Severity
Event
Time
Details
Local 1 Info User logged off 25/09/2010 03:52:56 Host:212.199.134.183,Peer:OSD1,Level:Admin
Local 1 Info Change server succeeded 25/09/2010 03:42:50 Server:Server 03
Local 1 Info Change server succeeded 25/09/2010 03:42:39 Server:Server 19
Local 1 Info Change server succeeded 25/09/2010 03:42:21 Server:Server 32
Local 1 Info Log on succeeded 25/09/2010 03:42:10 Host:212.199.134.183,Peer:OSD1,Level:Admin
Local 1 Info Log on succeeded 25/09/2010 03:42:01 OSD1
Local 1 Info Log on succeeded 25/09/2010 03:41:41 Host:212.199.134.183,Peer:OSD1,Level:Admin
admin Info User logged off 25/09/2010 03:33:14 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info Log on succeeded 25/09/2010 03:22:43 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info Log on succeeded 25/09/2010 03:22:23 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info User logged off 22/09/2010 05:51:48 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info Log on succeeded 22/09/2010 05:41:42 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
System Info System boot 22/09/2010 05:41:06 Version 2.1.0 Build(515)
admin Info Log on succeeded 22/09/2010 05:40:10 85.130.230.26
admin Info Log on succeeded 22/09/2010 05:33:30 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info User logged off 20/09/2010 10:50:46 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info Log on succeeded 20/09/2010 10:36:09 Host:212.199.134.183,Peer:85.130.230.26,Level:Admin
admin Info User logged off 15/09/2010 06:11:44 Host:212.199.134.183,Peer:212.199.134.130,Level:Admin
admin Info Change server succeeded 15/09/2010 05:55:56 Server:Server 02
admin Info Log on succeeded 15/09/2010 05:55:50 Host:212.199.134.183,Peer:212.199.134.130,Level:Admin
System Info System boot 15/09/2010 05:51:03 Version 2.1.0 Build(515)
Local 1 Warning IP changed 15/09/2010 05:50:21 Old:192.168.0.254,New:212.199.134.183
Local 1 Warning DG changed 15/09/2010 05:50:21 Old:192.168.0.1,New:212.199.134.161

Figure 60 – Events Log

5.2 Reloading the Events Log

As new events are constantly added to the log, you can reload the Events Log at any time.

➔ **To reload the Events Log:**

1. In the Events Log page (see Figure 60), in the toolbar, click Reload.

   The Events Log page is refreshed.

5.3 Saving the Events Log

You can download and save the Events Log to a .csv file. The file can then be viewed using Microsoft Excel or compatible software.

➔ **To save the Events Log:**

1. In the Events Log page (see Figure 60), in the toolbar, click Save As....

   The Save As window is displayed.

2. Type a name for the file, and click **Save**.

5.4 Clearing the Event Log

You can clear all the events in the log.

➔ **To clear the Events Log:**

1. In the Events Log page (see Figure 60), in the toolbar, click Clear All.

   A confirmation window appears.

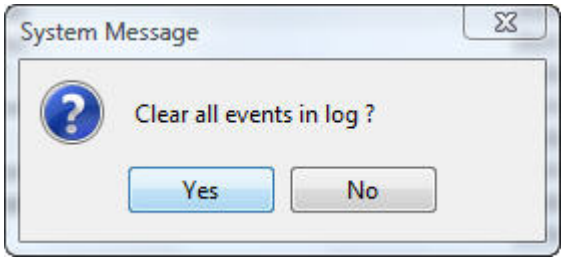


Figure 61 – Clear Events Confirmation Window

2. Click **Yes**.

   The Events Log is cleared.

6 Troubleshooting – Restoring Factory Settings

You can restore factory defaults from the Web configuration interface, as described in Section 3.13.3 on page 46. However, if you cannot access the GUI (for example, you have forgotten the Username or Password), you can restore factory defaults using a USB drive.

➔ **To restore factory defaults using a USB drive:**

1. In the root of the USB drive, create an empty file named "default".
2. Place the USB drive into one of the USB ports of the Smart 216/232 IP and restart it by power cycling it.

   The Smart 216/232 IP reboots and recognize the presence of the default file. It then restores the unit to the factory settings, erases this file, and reboots. After rebooting, the unit reverts to the factory settings.

7 Operating the Smart 216/232 IP Switching System Locally

This chapter explains how to operate the Smart 216/232 IP Switching system locally.

7.1 Displaying the OSD

➔ **To display the OSD:**

1. From the local keyboard, press the left **Shift** key twice.

   The OSD Main window appears.

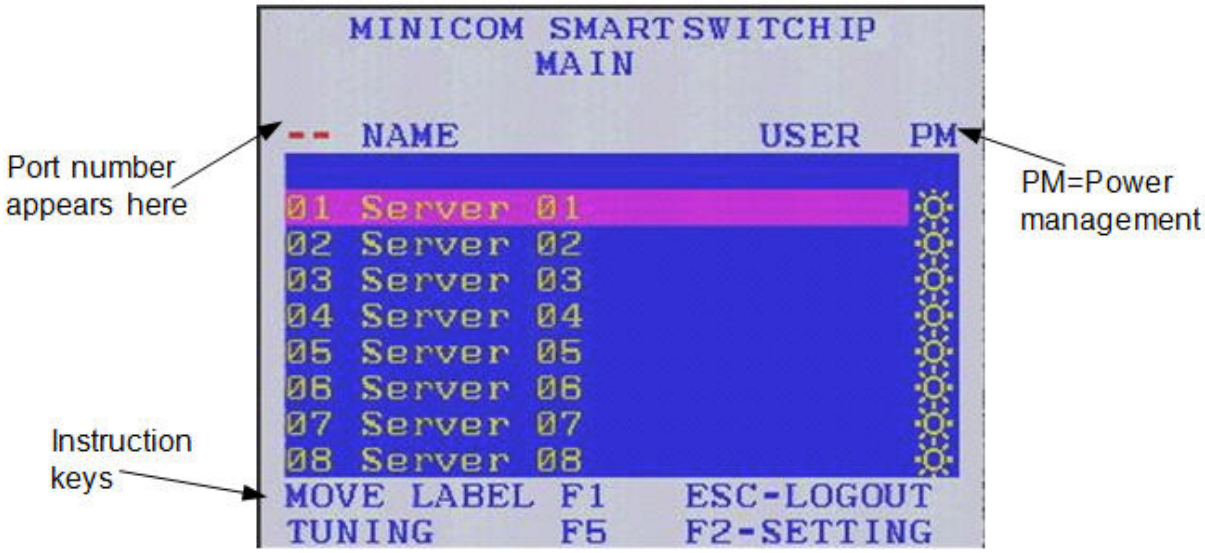


Figure 62 – OSD Main Window

Lines with the sun icons in the **PM** column show switched on active computers/servers. A switched off computer has no sun icon. When a server is busy, the entire line appears in red characters.

7.2 Navigating the OSD

You can navigate the OSD, as follows:

- To move up and down – Use the **Up** and **Down** arrow keys.
- To jump from one column to the next (when relevant) – Use the **Tab** key.
- To exit the OSD or return to a previous window within the OSD – Press **Esc.**

7.3 Selecting a Computer

➔ **To select a computer:**

1. Navigate to the desired computer line.

   OR

   Type the two-digit port number of the desired computer.

2. Press **Enter**.

   The selected computer is accessed. A Confirmation label appears showing which computer is accessed.

7.4 Power Managing a Server

You can power manage a server connected to a power management switch.

➔ **To power manage a server:**

1. Navigate to the line of the computer that you want to power manage.

   The Power Control dialog box appears.

Figure 63 – Power Control Dialog Box

If you change the OSD hotkey from Shift to Ctrl, the power management hotkey becomes left Ctrl, F12.

2. Use the arrow keys to navigate up and down, and press **Enter** to select the power option.

   A prompt appears.

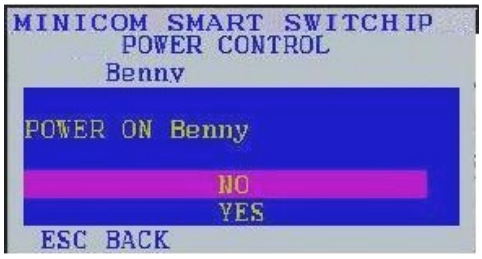


Figure 64 – Power Prompt

3. Select the desired option and press **Enter**.

   The power command is sent.

7.5 Moving the Confirmation Label (F1)

The Confirmation label appears briefly, showing which computer is currently accessed. You can position the Confirmation label anywhere on the screen.

➔ **To position the label:**

1. In the OSD Main window (see Figure 62), navigate to the desired computer using the **Up** and **Down** arrow keys.
2. Press **F1**.

   The selected screen image and Confirmation label appear.

3. Use the arrow keys to move the label to the desired position.
4. Press **Esc** to save and exit.

7.6 Tuning (F5)

You can tune the image of any computer screen from the Main window.

➔ **To adjust the screen image:**

1. In the OSD Main window (see Figure 62), navigate to the computer that you want to adjust.
2. Press **F5**.

   The screen image of the selected computer appears, together with the Image Tuning label.

Figure 65 – Image Tuning Label

3. Use the **Right** and **Left** arrow keys to adjust the image.
4. When the image is satisfactory, press **Esc**.

Picture quality is relative to distance. The further away a remote computer is from the Smart 216/232 IP, the lower the image quality, and the more tuning is required. Therefore, place the higher resolution computers closer to the Switch.

7.7 Configuring the OSD Settings (F2)

You can configure the following OSD settings:

- Network parameters
- OSD hotkey
- Keyboard Language

➔ **To configure the OSD settings:**

1. Press **F2**.

   The OSD Settings window appears.

Figure 66 – OSD Settings Window

In the Settings window, you can navigate downwards using the **Tab** key. At the bottom of the window, press the **Tab** key to go to the top of the window. Change

settings by typing in the selected area or by pressing the spacebar – whichever is relevant.

7.7.1 Changing the Network Parameters

You can configure the:

- Device IP address
- KVM.Net address

Configuring the Device IP Address

When a DHCP server is active on the same network to which Smart 216/232 IP is connected, the DHCP can provide automatic IP assignment. However, best practices recommend using MAC address reservations in the DHCP server to ensure that the IP address of the Smart 216/232 IP will not be changed.

Consult your Network Administrator regarding the use of the DHCP.

Selecting Automatic IP Address Assignment

➔ **To select automatic IP address assignment:**

1. In the OSD Settings window (see Figure 66), navigate to the **DHCP** line, and press the Space bar until **Enable** appears.

   The DHCP server that is active on the same network to which Smart 216/232 IP is connected, to provide automatic IP assignment.

Selecting Manual IP Address Assignment

➔ **To select manual IP address assignment:**

1. In the OSD Settings window (see Figure 66), navigate to the **DHCP** line, and press the Space bar until **Disable** appears.
2. Navigate to **IP Address**, and type the **IP address** for LAN 1 provided by your Network Administrator.
3. Similarly, navigate to **Subnet Mask** and **Default Gateway**, and type values for them.

Configuring AccessIT Centralized Management Settings

You can enable AccessIT centralized management, so that Minicom's AccessIT Centralized Management system remotely manages the Smart 216/232 IP unit.

➔ **To enable AccessIT Centralized Management:**

1. In the OSD Settings window (see Figure 66), navigate to the **KVM NET MANG** line, and press the Space bar until **Enable** appears.

2. Navigate to **KVM.NET ADD**, and modify the static IP address of the AccessIT Centralized Management Manager.

➔ **To disable AccessIT Centralized Management:**

1. In the OSD Settings window (see Figure 66), navigate to the **KVM NET MANG** line, and press the Space bar until **Disable** appears.

7.7.2 Changing the OSD Hotkey

By default, pressing **Shift, Shift** displays the OSD.

You can replace the OSD hotkey **Shift, Shift** with any of the following:

- **Ctrl, Ctrl**
- **Ctrl, F11**
- **Print Screen**

➔ **To change the hotkey:**

1. In the OSD Settings window (see Figure 66), navigate to the **Hotkey** line.
2. Press the Space bar to toggle between the available options.

From now on, you can press this new hotkey to display the OSD.

7.7.3 Changing the Keyboard Language

The keyboard language is preset to US English. You can change the keyboard language to French (FR) or German (DE).

This refers to the OSD keyboard language and not the computer keyboard language.

➔ **To change the keyboard language:**

1. In the OSD Settings window (see Figure 66), navigate to the **Keyboard Language** line.
2. Press the Space bar to toggle between the available options.

7.7.4 Inputting and Updating DDC Information (F10)

Display Data Channel (DDC) is a VESA standard for communication between a monitor and a video adapter.

The ROC emulates the DDC information to the connected computer.

When first installing the system, emulate the DDC information of the monitor connected to the Smart 216/232 IP switch into the memories of all connected ROCs.

➔ **To input the DDC information:**

1. From the OSD Settings window (see Figure 66), press **F10**.

   "Please wait" flashes a few times and disappears. The monitor's DDC information is sent to all ROCs.

You should update the DDC information in any of the following circumstances:

- When replacing the monitor connected to Smart 216/232 IP Switch
- When adding a new ROC to the system
- When reconnecting an existing ROC that was temporarily used in a different system

To update the DDC information, follow the steps in the procedure for inputting DCC information.

7.7.5 Saving Changes to Settings

➔ **To save changes to the settings:**

1. In the OSD Settings window (see Figure 66), press **Esc**.

   Settings are saved. The OSD Main window appears (see Figure 62).

8 Technical Specifications

Specification	Description
Operating systems	**Target server** – DOS, Windows, Novell, Linux, or SUN Solaris for PC **Client computer** – Windows 2000 or later with Internet Explorer 7.0 / Firefox 3.0 and later; Linux x86 with Firefox 3.0 and later
Resolution	**Target server** – Up to 1600 x 1200 @ 85 Hz **Client computer** – Recommended resolution should be higher than on target server
Distance from Switch to ROCs	Up to 30 m / 99 ft
Video and mouse synchronization	Both auto and manual modes
Security	SSL, high grade 256-bit AES encryption
Connections	**Ethernet** – RJ45 – 10/100 Mbit/sec autosensing **Serial** – RJ45 x 2 **Local KVM connection** – Screen HDD15; Keyboard/Mouse – 2 USB **Server** – RJ45
Weight	2.343 Kg / 5.165 lbs
Dimensions (H x D x W)	44 x 270 x 431 mm / 1.7 x 10.6 x 17"
Power input	100-240 VAC, 0.8 A, 50/60 Hz
Operating temperature	0°C to 40°C / 32° to 104°F
Storage temperature	-40°C to 70°C / -40°F to 158°F
Humidity	80% non-condensing relative humidity

Specification	ROC PS/2	ROC USB
Connections	**VGA** – HDD15 **KM** – MiniDin6 **System** – RJ45	**VGA** – HDD15 **KM** – USB **System** - RJ45
Power	From Keyboard port	From USB port
Product Weight	100 g / 0.20 lb	

Specification	ROC PS/2	ROC USB
Shipping Weight	172 g / 0.38 lb	
Dimensions (H x D x W)	65 x 25 x 25 mm / 2.6 x 0.98 x 0.98 in	

9 Video Resolution and Refresh Rates

Hz →	56	60	65	66	70	72	73	75	76	85	86
640x480		x		x	x	x		x		x	
720x400					x					x	
800x600	x	x				x		x		x	x
1024x768		x			x	x	x	x	x	x	
1152x864								x			
1152x900				x					x		
1280x720		x									
1280x768		x						x			
1280x960		x								x	
1280x1024		x				x		x	x	x	
1600x1200		x	x		x			x		x	

MINICOM
advanced systems